Freeform Search

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Term:

Display: 10 **Documents in Display Format:** - **Starting with Number** 1

Generate: ○ Hit List ◉ Hit Count ○ Side by Side ○ Image

Search Clear Interrupt

Search History

DATE: Saturday, September 24, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L14	L11 and 705/39	21	L14
L13	L11 and 705/44	9	L13
L12	L11 and 705.clas.	77	L12
L11	L10 and (central with controller or central near controller or central adj controller)	149	L11
L10	L9 and (internet or www or network or web)	1369	L10
L9	terminal and password and transaction and account and (identification or "id") and (bank with account or bank near account or bank adj account) and (funds or money)	1421	L9
L8	902/3	178	L8
L7	902/2	132	L7
L6	902/1	120	L6
L5	902.clas.	2099	L5
L4	705.clas.	36804	L4
L3	705/74	120	L3
L2	705/44	970	L2
L1	705/39	1676	L1

END OF SEARCH HISTORY

L12: Entry 63 of 77 File: USPT Jul 10, 2001

US-PAT-NO: 6260024
DOCUMENT-IDENTIFIER: US 6260024 B1

TITLE: Method and apparatus for facilitating buyer-driven purchase orders on a commercial network system

DATE-ISSUED: July 10, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Shkedy; Gary	New York	NY	10028	

APPL-NO: 09/ 203843 [PALM]
DATE FILED: December 2, 1998

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/37; 705/10, 705/28, 705/23, 705/26
US-CL-CURRENT: 705/37; 705/10, 705/23, 705/26, 705/28

FIELD-OF-SEARCH: 705/28, 705/10, 705/35, 705/26, 705/23, 705/25, 705/14, 705/44, 705/37, 380/25, 380/23

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4903201	February 1990	Wagner	
☐	5191613	March 1993	Graziano et al.	
☐	5794207	August 1998	Walker et al.	705/23
☐	5794219	August 1998	Brown	
☐	5835896	November 1998	Fisher et al.	

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
411748	June 1991	EP	

OTHER PUBLICATIONS

Murray, John E Jr, When a contract is not a contract, PP 1-3, Dec. 1996.*
Wall street Journal, Eastern edition, PP 1-3, Apr. 1991.*

Structuring an Acquistion Strategy, Green, Janet M, PP 1-6, Dec. 1992.*
Like going to the grocery store, Credit Card Management, James J Daly, PP 1-6, Aug. 1997.*
The buyer can't lose, Purchasing, Murray John, PP 1-3, Feb. 1997.*
Search Report of International Appln. No. PCT/US99/28507.

ART-UNIT: 212

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Tesfamariam; Mussie K.

ABSTRACT:

Systems and methods are described for providing a global bilateral buyer-driven system for creating binding contracts by incorporating various methods of communication, commerce and security for the buyers and the sellers. Individual buyers purchase requirements are aggregated into a single collective purchase requirement and sellers are located willing to bid on the collective purchase requirement. A central controller facilitates the buyer/seller transaction by fielding binding offers from buyers, aggregating those offers into group (i.e. pooled) offers and communicating those group offers globally in a format which can be efficiently accessed and analyzed by potential sellers. This system can also effectuate performance of resulting contracts, resolve disputes arising from those contracts, and maintain billing, collection, authentication, and anonymity. The methods disclosed are applicable to any commerce situation involving buyers and sellers.

37 Claims, 17 Drawing figures

Previous Doc Next Doc Go to Doc#

L12: Entry 63 of 77 File: USPT Jul 10, 2001

DOCUMENT-IDENTIFIER: US 6260024 B1
TITLE: Method and apparatus for facilitating buyer-driven purchase orders on a commercial network system

Abstract Text (1):
Systems and methods are described for providing a global bilateral buyer-driven system for creating binding contracts by incorporating various methods of communication, commerce and security for the buyers and the sellers. Individual buyers purchase requirements are aggregated into a single collective purchase requirement and sellers are located willing to bid on the collective purchase requirement. A central controller facilitates the buyer/seller transaction by fielding binding offers from buyers, aggregating those offers into group (i.e. pooled) offers and communicating those group offers globally in a format which can be efficiently accessed and analyzed by potential sellers. This system can also effectuate performance of resulting contracts, resolve disputes arising from those contracts, and maintain billing, collection, authentication, and anonymity. The methods disclosed are applicable to any commerce situation involving buyers and sellers.

Brief Summary Text (3):
The method and apparatus of the present invention relates to electronic commerce network applications and, more particularly, to a system and method for facilitating a transaction between a plurality of buyers, an intermediary, and a plurality of sellers over an electronic network.

Brief Summary Text (5):
The purchase of goods and services in an electronic/telephone network, such as the Internet has gained acceptance by a large segment of the population. Market forecasts indicate that E-commerce will gain widespread usage as a medium for commercial transactions among buyers and sellers. Numerous Internet purchase websites are currently available. The majority of these sites may be classified as seller driven. The traditional retail commerce model is one example of a seller driven protocol characterized by a product offer by a large number of manufacturers to a mass market of consumers via a range of intermediary retail channels (sellers). The retail model is said to be seller driven in that a seller must utilize various methodologies, including advertising, packaging, and pricing, to attract potential buyers. Further, in a seller driven model the seller assumes all risks and costs associated with consummating a sale.

Brief Summary Text (6):
With an ever increasing number of retailers implementing electronic commerce solutions, such as electronic malls, catalogs and auction houses, the seller driven protocol is carried over into that realm. In the electronic commerce model, it is undisputed that the customer exercises a greater degree of control over the transaction as compared to the conventional retail model, however, it is equally undisputed that the protocol remains primarily seller driven.

Brief Summary Text (10):
Buyer-driven protocols are available on the Internet. (See, e.g. www.priceline.com) . These protocols allow buyers to define a conditional purchase offer. The buyer selects the particular item he wishes to purchase, adds any conditions he wishes to place on the purchase and specifies a price at which he will purchase. He then transmits this conditional purchase offer to a central computer. Suppliers then search a list of conditional purchase offers and select the ones they are willing to bind. In effect, the site owner provides a mechanism for binding the buyer and seller to an electronic contractual agreement.

Brief Summary Text (16):

There is also a need for a third party to administer such bilateral multi buyer-driven system. The third party can administer an Internet site where buyers can aggregate their orders into a large pooled purchase order. Also, this third party can act as an agent for all the buyers and achieve economies of purchasing usually only achieved by large retailers or corporations. Also, a central site for the global purchase order facilitates a venue for sellers to search for appropriate orders to bid on.

Brief Summary Text (27):
In one aspect of the invention, a method for using a computer acting as an intermediary to facilitate a transaction between a plurality of buyers and at least one seller comprises the steps of: a buyer determining an item or service to be purchased, the buyer inputting a conditional purchase order to a central controller (i.e. intermediary party) for the item or service, receiving a maximum offer price in response to the conditional purchase order from the central controller, the buyer either accepting or rejecting the maximum offer price from the central controller. If the buyer accepts the maximum offer price, the buyers' conditional purchase order is combined into a pooled purchase order with other buyers. The pooled purchase order is then made available to sellers to bid on. Any sellers interested in the pooled purchase order will submit a bid including a bid price that is responsive to the conditional pooled purchase order, including the maximum offer price. A seller will be selected whose bid is the best, e.g. lowest price. Payment can be provided by the intermediary to the seller having the lowest bid.

Drawing Description Text (2):
FIG. 1 is a block diagram illustrating an electronic network in accordance with an embodiment of the present invention.

Drawing Description Text (3):
FIG. 2 is a block diagram showing an embodiment of the central controller.

Drawing Description Text (8):
FIG. 6 illustrates the acceptance of a forward purchase order and the creation of a pooled purchase order by the central controller in accordance with an embodiment of the present invention.

Drawing Description Text (10):
FIG. 9 illustrates the selection of the optimal bid by the central controller on a pool date in accordance with an embodiment of the present invention.

Detailed Description Text (3):
Referring now to FIGS. 1 and 2a, and in particular to FIG. 1, in a preferred embodiment, an electronic network including a central controller 200 is shown. The network facilitates communications between a plurality of buyers and a plurality of sellers through an intermediary (i.e. central controller 200). FIG. 1 illustrates a plurality of buyers electronically coupled to central controller 200 with buyer modems 450, the central controller 200 is electronically coupled to a plurality of seller through seller modems 350 and sellers 300. Each of the plurality of buyers who wish to make purchases independently access the central controller 200 to create forward purchase orders(FPOs) to submit their purchase orders for items and/or services. The central controller 200 is preferably located at a remote server.

Detailed Description Text (4):
FIG. 2a illustrates the steps associated with the creation, transmission and inclusion of an FPO 100 into the PPO database 265. At step 40, a buyer selects the category of goods or service to be purchased. At step 42, the buyer selects the particular item or service in the category. At step 44, the buyer 16 adds a quantity specifier along with any other required buyer specified conditions. At step 46, a buyer will specify along with item, quantity, and buyer identification data, the pool date (i.e. seller bidding date) he wishes to participate in and an outside delivery date. The pool date represents the specific date at which the central controller (intermediary) 200 will make the PPO 110 available to the sellers for bidding. A buyer will typically have a choice of two or more pool dates from which to choose. He must, however, select only a single pool date into which his FPO 100 will be included. If his FPO comprises multiple categories of goods, he could, however, provide a single pool date per category.

Detailed Description Text (5):

At step 48, the buyer is prompted for possible additional items or services that he wishes to purchase. If so, steps 40-46 are repeated for each additional item or service to be purchased, otherwise at step 50, the buyer attaches his user identification to the FPO and transmits the FPO to the central controller 200.

Detailed Description Text (7):
At step 54, the central controller 200 determines a maximum offer price for the submitted FPO 100 and transmits that price back to the buyer. The central controller 200 may add legal language to the FPO 100 to make it explicit to the buyer that should the buyer accept the maximum offer price he will be entering into a binding agreement. Step 56 is a determination step for the buyer 16 to decide whether he is willing to accept the maximum offer price provided by the central controller 200. If not, the FPO 100 creation process terminates at step 58. Otherwise, if the buyer accepts the maximum offer price his FPO 100 will be included in the pool purchase order at step 60 by transmitting his intention to accept to the central controller 200. The buyer has now consented to entering into a legally binding contract with the intermediary and will accept the best price that the intermediary determines in the bidding process subject to the condition that the buyer will pay no more for the item or service than the stipulated maximum offer price.

Detailed Description Text (8):
At step 62, before adding the FPO 100 to a PPO 110, the central controller 200 authenticates the buyer's identification number against a buyer database. The central controller 200 may require that the buyer provide a credit card number and may also ensure that the buyer has sufficient credit available to cover the purchase price specified in the FPO 100 by contacting a credit card clearinghouse. Once a buyer is authenticated and credit worthy, at step 64, the central controller 200 assigns a unique tracking number to the FPO 100 and adds it to the pooled purchase order database. At step 66 the central controller 200 publishes or displays the PPO 110 in a manner accessible by potential sellers. For example, on a website on the Internet. The central controller may display the PPO database 265 by category to make it easier for potential sellers to identify PPOs relevant to their products. Furthermore, before displaying a PPO 100 to a seller, the central controller 200 could add legal language to make it explicit to the seller that he is entering into a binding contract. Thus, a seller could log onto the website, for example, and see a listing of PPO categories. The seller could then choose a particular category and have the ability to browse PPOs which correspond to that category. In one embodiment, the seller may be required to provide qualifications in order to view the PPOs of a given category.

Detailed Description Text (9):
If after reviewing a particular PPO a potential seller wishes to make a bid, the seller communicates his intent to the central controller 200. The central controller 200 then time-stamps the message from the seller and authenticates the identity of the seller and his capacity to deliver the goods defined by the PPO. The system then verifies that the particular PPO is still "active" and capable of being bid on. If a seller bids on an active PPO, a unique tracking number is assigned to the seller's bid and the bid is stored in a database. The seller has now entered into a legally binding contract with the intermediary.

Detailed Description Text (10):
In the event that a seller is awarded the bid, the central controller 200 will send a purchase confirmation to the seller. Once the transaction has been completed i.e. the goods have been delivered, the intermediary will pay the seller preferably in a single payment for the total cost of the PPO. This would represent substantial savings to the seller in transaction costs and may encourage him to lower his bid. The payment may be made by the intermediary in any number of ways including using a credit card, electronic funds transfer, corporate purchasing card, corporate purchase order etc.

Detailed Description Text (11):
Under the present invention, communications between the various parties may be transmitted via numerous means including a world-wide-web interface, personal digital assistant (PDA), electronic mail, voice mail, facsimile, or postal mail. Other means not explicitly enumerated herein but known to one ordinarily skilled in the art are also within the scope of the invention.

Detailed Description Text (12):
In another embodiment, as a substitute for making the PPO database 265 globally available to a

plurality of sellers, the central controller 200 could instead pro-actively contact potential sellers to explicitly request them to bid on the PPOs in the PPO database 265.

Detailed Description Text (13):
The central controller 200 manages the payment system between the buyer and seller automatically. Various methods of payment may be utilized by the invention including credit cards, personal checks, electronic funds transfer, debit card, money orders, corporate purchasing cards, smart cards, digital cash and micropayments. The payment system may also involve the use of an escrow account associated with the buyer wherein funds advanced by the buyer to cover the purchase of a desired good can be kept pending delivery of the goods by the selected seller 20. Moreover, the timing of payment to the seller can be varied.

Detailed Description Text (14):
The present invention can also be practiced in off-line embodiments. Instead of using electronic mail or web-based servers, buyers and seller may communicate with the central controller 200 via telephone, facsimile, postal mail, or another off-line communication tool. For example, buyers may use telephones to create FPOs 100 (with or without the assistance of live agents) and potential seller may use a telephone to browse and bid on PPOs.

Detailed Description Text (15):
Cryptographic protocols are provided to authenticate the identity of buyers and/or sellers and verify the integrity of buyer and seller communications with the central controller 200. The use of cryptography, smart cards and biometrics can make it significantly more difficult for unauthorized persons to tamper with the system by passing themselves off as legitimate buyers or sellers or eavesdropping on system communications.

Detailed Description Text (16):
In another on-line embodiment, either buyer or the seller or the central controller 200 could use intelligent software agents to accomplish all or some of the buyer/seller communications with the central processor. Thus the central processor provides a meeting place for such agents to congregate and aggregate. The central controller 200 could then create a super agent that would be used to find the most competitive bid for the pool.

Detailed Description Text (17):
In one embodiment of the present invention buyers could indicate a minimum discount off the maximum offer price provided by the central controller 200 that a buyer would be willing to accept. The seller would then be notified of a maximum price he had to beat in order to bid.

Detailed Description Text (20):
One embodiment of the present invention divides the functionality of the central controller 200 into three components and embodies them in three separate servers: an operations server, a certificate authority, and a settlement server. The certificate authority authenticates the identity of buyers and sellers while the settlement server verifies their ability to pay or deliver goods. The operations server posts FPOs, PPOs and bids relying upon messages from the other two servers for validation. This configuration allows greater specialization of the servers.

Detailed Description Text (22):
In another embodiment of the present invention the central controller 200 does not specify a maximum offer price, but would instead specify a commission and/or a cancellation fee to the buyer for entering the pool. The specification of the fees satisfies the legal requirement for consideration. This embodiment could be extremely useful for the intermediary to negotiate services for the pool. An example of this could be the negotiation of medical benefits for a large pool of small businesses.

Detailed Description Text (23):
Another embodiment of the present invention does not require a transfer of funds from a buyer to a seller. Instead, the system may be used to consummate a contract involving an exchange of goods, services, or other non-monetary consideration.

Detailed Description Text (24):
A further embodiment of the present invention includes a mechanism for resolving disputes between buyers and sellers arising out of agreements consummated using the system. The parties may be required in FPOs and bids to stipulate to binding arbitration and may be assisted in the

arbitration process by the central controller 200. The central controller 200 may serve as an arbitrator or may refer the dispute to a third-party arbitrator for resolution.

Detailed Description Text (25):
The present invention is a highly effective bilateral multi buyer-driven commerce system which improves the ability of buyers to achieve the purchasing power heretofore made exclusively available to very large organizations. The present invention provides numerous unique advantages including anonymity. For numerous privacy and competitive reasons, buyers and sellers often prefer not to have their identities revealed to the general public when engaging in commercial transactions. The present invention effectuates the anonymity of buyers and sellers through the use of identification numbers stored in a database secured by the central controller 200.

Detailed Description Text (26):
The method and apparatus of the present invention will now be discussed with reference to FIGS. 1,2,3, and 4. In a preferred embodiment, the present invention includes central controller 200, seller interface 300, buyer interface 400, and associated databases. The present invention receives forward purchase orders from buyers, creates pooled purchase orders, makes the pooled purchase orders available for viewing by potential sellers, and allows sellers to bid on them. A buyer is able to communicate his commitment to the pool. The intermediary is able to communicate its ability to follow through on an order to a seller, giving the seller confidence that if he can produce the goods at the best price, the intermediary (the buyer pool) has the ready capacity to pay.

Detailed Description Text (27):
The system architecture of a preferred embodiment of the apparatus and method of the present invention is illustrated with reference to FIGS. 1 through 4. As shown in FIG. 1, an apparatus of the present invention comprises seller interface 300, central controller 200, and buyer interface 400 (collectively the "nodes"). Each node is connected via an Internet connection using a public switched phone network, such as those provided by a local or regional telephone operating company. Connection may also be provided by dedicated data lines, cellular, Personal Communication Systems ("PCS`), microwave, or satellite networks. Other embodiments may use other known means of communication not enumerated herein. Seller interface 300 and buyer interface 400 are the input and output gateways for communications with central controller 200.

Detailed Description Text (29):
As shown in FIG. 2, central controller 200 includes central processor (CPU) 205, cryptographic processor 210, RAM 215, ROM 220, payment processor 230, clock 235, operating system 240, network interface 245, and data storage device 250.

Detailed Description Text (30):
A conventional personal computer or computer workstation with sufficient memory and processing capability may be used as central controller 200. The memory may be in the form of a hard disk, CD ROM, or equivalent storage medium. The memory stores data including program codes for causing the processor to operate the steps and functions of the present invention. In one embodiment it operates as a web server, both receiving and transmitting FPOs 100 generated by buyers. Central controller 200 is capable of high volume transaction processing, performing a significant number of mathematical calculations in processing communications and database searches. A Pentium II class processor, commonly manufactured by Intel Inc., may he used for CPU 205.

Detailed Description Text (31):
An MC68HC16 micro-controller, commonly manufactured by Motorola Inc., or any equivalent may he used for cryptographic processor 210. Cryptographic processor 210 supports the authentication of communications from buyers and sellers, as well as allowing for anonymous transactions. Ideally, cryptographic processor 210 may also be configured as part of CPU 205. Other commercially available specialized cryptographic processors include VLSI Technology's 40 MHz VMS110.

Detailed Description Text (32):
Referring again to FIG. 2, payment processor 230 comprises one or more conventional microprocessors (such as the Intel Pentium II), supporting the transfer and exchange of payments charges, or debits, attendant to the method of the apparatus. Payment processor 230

may also be configured as part of CPU 205. Processing of credit card transactions by payment processor 230 may be supported with commercially available software, such as the Secure Webserver manufactured by Open Market, Inc. This server software transmits credit card numbers electronically over the Internet to servers located at the Open Market headquarters where card verification and processing is handled. Their Integrated Commerce Service provides back-office services necessary to run Web-based businesses. Services include on-line account statements, order-taking and credit card payment authorization, credit card settlement, automated sales tax calculations, digital receipt generation, account-based purchase tracking, and payment aggregation for low-priced services.

Detailed Description Text (33):
Data storage device 250 may include hard disk magnetic or optical storage units, as well as CD-ROM drives or flash memory. Data storage device 250 contains databases used in the processing of transactions in the present invention. These include buyer database 255, seller database 260, FPO database 265, PPO database 267, seller bidding database 270, purchase confirmation database 275, contract detail database 280, payment database 285, cryptographic key database 290, and audit database 295. In a preferred embodiment database software such as Oracle8, manufactured by Oracle Corporation, is used to create and manage these databases. Data storage device 250 also stores information pertaining to intermediary account 286, buyer account 297, seller account 298, and escrow account 299.

Detailed Description Text (34):
Buyer database 255 maintains data on buyers with fields such as name, address, telephone number, credit card number, ID number, social security number, electronic mail address, smart card ID, credit history, public/private key information etc. This information is obtained when the buyer first registers with the system, or immediately prior to posting his first FPO 100. Buyer database 255 also contains the tracking number of each FPO 100 generated by the buyer, and the tracking number of each pooled order 110 that comprises the buyer's FPOs 100.

Detailed Description Text (35):
Seller database 260 maintains data on sellers with fields such as name, contact information, public/private key information, payment preferences, type of business, and goods sold. Contact information comprises a phone number, web page URL, pager number, telephone number, electronic mail address, voice mail address, facsimile number, or any other way to contact the seller. It also contains data regarding the items the seller can deliver with fields such as item ID, current price, restrictions on sale and discount schedule for large quantities etc. Upon registration, the seller may be required to demonstrate evidence of ability to deliver on goods in each category. A distributor, for example, might submit a listing of the items he provides so that central controller 200 can quickly determine whether the distributor is capable of satisfying a given PPO 110.

Detailed Description Text (36):
Item database 262 maintains data on all items that can be added to FPOs by buyers. It has fields such as item ID, description, category, photo (if applicable), ceiling price etc. This database is the catalog of items available for sale by sellers. If an item does not exist, buyers may be able to add them to the database.

Detailed Description Text (37):
FPO database 265 tracks all FPOs 100 with fields such as status, tracking number, date, time, subject, ceiling price, pool date, conditions, and buyer identification number. This database is valuable in the event of disputes between buyers and the intermediary regarding payment, because details of the FPO contract can be produced.

Detailed Description Text (38):
PPO database 267 tracks all PPOs 120 with field such as status, pool date, item ID, PPO tracking number, FPO tracking number, quantity, ceiling price etc. This database is also valuable in the event of disputes between sellers and intermediary as it contains all the details of the PPO contract that can be produced on request.

Detailed Description Text (39):
Sellers bidding database 270 tracks all seller bids 115 with fields such as seller name, seller ID number, date, time, seller bid tracking number, and associated PPO tracking number.

Detailed Description Text (40):

Purchase confirmation database 275 tracks the messages sent to the buyer and seller confirming completed transactions. Fields include buyer name, buyer ID number, seller name, seller ID number, purchase confirmation tracking number, and associated PPO tracking number.

Detailed Description Text (42):
Payment database 285 tracks all payments made by the buyers with fields such as buyer name, buyer ID number, amount of payment, and associated FPO tracking number. This database may also store credit card or smart card numbers of buyers.

Detailed Description Text (45):
Intermediary Account Database 296 tracks all payments made to and by the intermediary. Buyer payments for FPOs 100 may be sent to this account. This account may be a pointer to account data stored at the intermediary's bank.

Detailed Description Text (46):
Buyer account 297 tracks all information pertaining to the buyer's account with fields such as buyer's name, bank and credit account numbers, and debit or credit transactions. This account may be a pointer to account data stored at the buyer's bank.

Detailed Description Text (47):
Seller account 298 tracks all information pertaining to the seller's account with fields such as seller's name, bank and credit account numbers, and debit or credit transactions. Buyer payments for FPOs 100 may be sent to this account.

Detailed Description Text (48):
Escrow account 299 is an account which temporarily holds buyer funds before they are transferred either to the intermediary or the sellers' account 298.

Detailed Description Text (49):
Network interface 245 is the gateway to communicate with buyers and sellers through respective buyer interface 400 and seller interface 300. Conventional internal or external modems may serve as network interface 245. Network interface 245 supports modems at a range of baud rates from 1200 upward, but may combine such inputs into a TI or T3 line if more bandwidth is required. In a preferred embodiment, network interface 245 is connected with the Internet and/or any of the commercial on-line services such as America Online, IBM Global Network, CompuServe, or Prodigy. This allows buyers and sellers access from a wide range of on-line connections. Several commercial electronic mail servers include the above functionality. Microsoft Exchange Server 5.5 is a secure server-based electronic mail software package designed to link people and information over enterprise networks and the Internet. The product utilizes open standards based on Internet protocols. Users can exchange messages with enclosures such as files, graphics, video and audio. Alternatively, network interface 245 may be configured as a voice mail interface, web site, BBS, or electronic mail address.

Detailed Description Text (50):
While the above embodiment describes a single computer acting, as central controller 200, those skilled in the art will realize that the functionality can he distributed over a plurality of computers. In one embodiment, central controller 200 is configured in a distributed architecture, wherein the databases and processors are housed in separate units or locations. Some controllers perform the primary processing functions and contain at a minimum RAM, ROM, and a general processor. Each of these controllers is attached to a WAN hub, which serves as the primary communication link with the other controllers and interface devices. The WAN hub may have minimal processing capability itself, serving primarily as a communications router. Those skilled in the art will appreciate that an almost unlimited number of controllers may be supported. This arrangement yields a more dynamic and flexible system, less prone to catastrophic hardware failures affecting the entire system. The certificate authority embodiment provides more details of such a distributed environment describing operations server 160, certificate authority 165, and settlement server 170. The hardware of these servers would be configured similarly to that described for central controller 200.

Detailed Description Text (51):
FIGS. 3 and 4 describe seller interface 300 and buyer interface 400, respectively. In an exemplary embodiment they are both conventional personal computers having an input device, such as a keyboard, mouse, or conventional voice recognition software package; a display device, such as a video monitor a processing device such as a CPU; and a network interface such as a

modem. These devices interface with central controller 200. Alternatively, seller interface 300 and buyer interface 400 may also be voice mail systems, PDAs, or other electronic or voice communications systems. As will be described further in the following embodiments, devices such as fax machines or pagers are also suitable interface devices.

Detailed Description Text (54):
Data storage device 360 is a conventional magnetic-based hard disk storage unit such as those manufactured by Conner Peripherals or Maxtor. Message database 370 may be used for archiving seller bids 115, while audit database 380 may be used for recording payment records and communications with central controller 200.

Detailed Description Text (56):
There are many commercial software applications that can enable the communications required by seller interface 300 or buyer Interface 400 the primary functionality being message creation and transmission. Eudora Pro manufactured by Qualcomm Incorporated, for example, provides editing tools for the creation of messages as well as the communications tools to route the message to the appropriate electronic address. When central controller 200 is configured as a web server, conventional communications software such as the Netscape Navigator web browser, from Netscape Corporation or Internet Explorer, from Microsoft may also be used. The buyer and seller may use these browsers to transmit FPO 100 or seller bids 115. No proprietary software is required.

Detailed Description Text (57):
In a preferred embodiment of the present invention, communications between buyers and sellers take place via electronic networks, with central controller 200 acting as a web server. The buyer logs on to central controller 200, selects the items he wishes to purchase, accepts the maximum price given by the central controller 200 and thereby creates FPO 100, and then disconnects from the network. PPO 110 is then created and made available to potential buyers by posting PPO 110 on the webpage of central controller 200. Periodically, the central controller 200 checks the databases to determine the optimal bid on PPOs 110. Seller bids 115 are transmitted electronically to central controller 200. When the optimal bid has been determined, the central controller contacts the buyer and the seller to indicate that they are mutually bound . Central controller 200 may transfer the intermediary credit card information to the seller as soon as the optimal bid on PPO 110 has been determined.

Detailed Description Text (58):
With reference to FIG. 5, there is described the process by which the buyer formulates FPO 100. At step 500, the buyer logs on to central controller 200 using buyer modem 450 of buyer interface 400, establishing a communication link. It should be noted that the buyer might be an individual, a corporation, a partnership, government or any other entity. In one embodiment, central controller 200 has a page on the World Wide Web, allowing the buyer to provide information through the interface of conventional web browser software such as Netscape Navigator, manufactured by Netscape, Inc or Internet Explorer, manufactured by Microsoft. At step 505, the buyer selects the category of the goods he wants to purchase by selecting from a list of possible categories. As shown in box 507 categories might include office supplies, automobiles, computers, mutual funds, stocks, airline tickets, hotel rooms, rental cars, insurance, mortgages, clothing, etc. After the category is selected, in step 510 the buyer than selects a particular item from that category. As shown in box 512, this might be a Cross roller pen, 1997 Ford Taurus GL with A/C package, a Dell Dimension XPS R450 Pentium II Processor at 450 MHz, a Fidelity S&P Index fund, IBM stock, a flight from New York to London etc. At step 520 a form is displayed on video monitor 430 of buyer interface 400 (Note steps 505 and 510 could also be accomplished in the same way). This form is an electronic contract with selection fields and/or a number of blanks to be filled out by the buyer, with each blank representing a condition of FPO 100.

Detailed Description Text (61):
At step 530, the central controller retrieves the pricing of the item from the item database 262 and creates a web page with the buyer selection, a place to indicate quantity and delivery date and the ceiling price and transmits it to the web browser of the buyer. At step 540 the buyer enters the quantity he requires and the delivery date into the appropriate fields. If the buyer has completed shopping he proceeds to step 560 else he can return to step 505 and select the category of his next purchase.

Detailed Description Text (62):

At step 560 the buyer attaches his name or a unique user ID number to FPO 100. This ID number is received from central controller 200 when the buyer registers for the service, or is chosen by the buyer and then registered with central controller 200 by phone. Central controller 200 maintains a database of buyer ID numbers in buyer database 255, and issues (or allows) only unique numbers. If less security is required, the user's telephone number or social security number could serve as the ID number since it has the advantages of being both unique and easily remembered. If additional security is required, those procedures described in the cryptographic embodiment may be implemented.

Detailed Description Text (63):
At step 570, the buyer is presented with a form (similar to method described above) with a selection of pool dates for each category he has selected. The pool dates define the particular day on which sellers will be allowed to place bids on PPOs. Pool dates would take place at regular intervals, typically once a week, but depending on demand could be more or less frequent. At this step the buyer selects the pool date he wishes to participate in. This gives the buyer the opportunity to maximize the effectiveness of pooling his FPO 100 to form a PPO 110. If he selects a pool date with the largest volume of FPOs 100, he is more likely to receive a better bid on the selected item represented by his individual FPO 100. At step 580 the central controller now forms the PPO. At this step, legal language is added to the FPO to form a complete FPO 100. The legal language is pulled from contract detail database 280, which stores a plurality of paragraphs. These paragraphs are linked together with the above contract elements to form a complete FPO 100.

Detailed Description Text (64):
Once the above elements have been developed, the buyer transmits them to central controller 200 at step 590. The buyer does this by clicking on a "send" button located on the screen in which he entered the terms of FPO100.

Detailed Description Text (65):
Instead of a World Wide Web based interface, buyers may also transmit FPO 100 data via other means including electronic mail, PDAs, EDI, voice mail, facsimile, or postal mail transmissions. With voice mail, the buyer calls central controller 200 and leaves FPO 100 in audio form. These FPOs 100 may be transcribed into digital text at central controller 200, or aggregated in multiple formats and made available to potential sellers in the same multiple formats. In a postal mail embodiment, central controller 200 acts more like a aggregator and router, collecting FPOs 100 and forming PPO 110 then directing PPOs 110 to the potential sellers, creating multiple copies of PPO 100 if necessary. PPO 110 may also be posted to bulletin boards or web pages operated by central controller 200. Central controller 200 supports a plurality of transmission methods, allowing for a wide variety of formats of FPOs 100 and PPOs 110. Some formats may be changed, however, before further processing by central controller 200. FPOs 100 transmitted by mail in paper form, for example, may be scanned-in and digitized, using optical character recognition software to create digital text and then used to create PPO 110. These embodiments are more fully described in the off-line embodiment described later.

Detailed Description Text (66):
Referring now to FIG. 6, FPO 100 is received and checked to see that sufficient credit is available to cover the ceiling price of FPO 100, before FPO 100 is added to PPO 110. At step 600, central controller 200 extracts price and expiration date information from FPO 100. At step 605, payment processor 230 submits a pre-authorization of the total ceiling price of FPO 100 to the credit card clearinghouse. This serves to "lock up" a portion of the available credit on the buyer's credit card, preventing him from using up this credit while FPO 100 is still active. At step 620, the credit card clearinghouse responds to the pre-authorization. Indicating whether sufficient credit is available. If sufficient funds are not available to cover the price of FPO 100, another credit card number is requested from the buyer at step 610. Once an additional credit card number has been transmitted central controller 200 then resubmits the pre-authorization at step 605. At step 620, the expiration date of the credit card is checked to see if it will expire before the pool date. If it will expire another credit card is requested and the pre-authorization process begins again.

Detailed Description Text (67):
If all is well, the FPO is accepted at step 630. At step 640 a unique tacking number is added to the FPO 100. The central controller 200 time-stamps FPO 100 at step 650 sets the status to "active" and stores FPO 100 in the FPO database 265. FPO database 265 contains a record for the

FPO 100 and a record for each item in the FPO 100. The FPO record contains fields such as status, tracking number, time-stamp and buyer ID. The status field has values of "pending," "active," "expired,` and "completed." A status of "pending", means that the FPO cannot currently be added into a PPO. Either, central controller 100 is still processing it, or the buyer has temporarily suspended it, or it is part of a multiple step signing key. An "active" FPO 100 is available to be added to a PPO. An "expired" FPO 100 can no longer be used. FPO 100 that have been bid and sold by a seller have a status of "completed." A record for an item of in FPO 100 has fields such item ID, a FPO tracking number, quantity, ceiling price and other conditions added by the buyer.

Detailed Description Text (68):
After being stored at step 670, FPO 100 may go through a series of processing steps. One step, if necessary, is language translation. The system may either create a standard language that all FPO 100s must be written in, or translate them to the a common PPO language. This translation is provided by language experts at central controller 200, or by automatic translation software such as Systran Professional 2.0, manufactured by Systran Software Inc. Fourteen bi-directional language combinations are available, including English to/from French, Italian, German, Spanish, Portuguese, Chinese, Russian and Japanese. Another step, if necessary, is to edit for spelling or grammatical errors. FPO 100 might also be reviewed for clarity. Any FPO 100 with an unclear term or condition would be returned to the buyer for clarification. A buyer adding an unintelligible condition might have FPO 100 returned for clarification or correction.

Detailed Description Text (69):
An example of a pooling process performed by the intermediary (central controller) 200 is now described. Buyer A wishes to purchase two dozen BIC medium point black roller ball pens for a maximum price of $5.00 per dozen. Buyer B wishes to purchase one dozen BIC medium point black roller ball pens for $5.00 per dozen, one dozen BIC medium point blue roller ball pens for $4.00 per dozen and one dozen pencils at $2.00 per dozen. The pooling or aggregation process adds the two FPOs to form a combined PPO 110 of three dozen BIC medium point black roller ball pens at $5.00 per dozen, one dozen BIC medium point blue roller ball pens at $4.00 per dozen and one dozen pencils at $2.00 per dozen. In another embodiment, the PPO 110 would be three dozen BIC medium point black roller ball pens, one dozen BIC medium point blue roller ball pens and one dozen pencils for a maximum price of $21.00.

Detailed Description Text (70):
Referring again to FIG. 7 the items of the FPO 100 are extracted from the FPO 100 at step 680. At step 690 these items are posted to the PPO database 267. The PPO database contains a record for each PPO 110 and a record for each item in the PPO. The PPO record contains fields such as status, tracking number, time-stamp, pool date and category. The status field has values of "pending," "active," "expired,` and "completed." A status of "pending", means that the PPO cannot currently be bid on by a seller. Either, central controller 100 is still processing it, or it has been closed to bidding. An "active" PPO 110 is available to be bid on by potential sellers. An "expired" PPO 110 can no longer be bid on. PPO 110 that have been bid and sold by a seller have a status of "completed." A record for an item of in PPO 110 has fields such item ID, a FPO tracking number, quantity, ceiling price and other conditions added by the buyer.

Detailed Description Text (71):
After being stored at step 690, PPO 110 may go through a language translation step. The system may either create a standard language that all PPO 110s must be displayed in, or translate them to the language most appropriate for the particular seller. This translation is accomplished the same way as described above for FPOs 100. The posting of PPO 110 to the database with appropriate categories allows central controller 200 to display PPO 110 only to the most appropriate sellers. In a World Wide Web environment, central controller 200 has a web page for each possible category. Thus all PPOs 110 requesting office supplies would be displayed on the office supply web page. This makes it much easier for potential sellers to find appropriate PPOs 110 they might want to bid on as they can go right to the category whose goods they can provide. In an alternative embodiment, PPO 110 is electronically mailed to potential sellers, either individually or in groups. Potential sellers could elect to receive all PPOs 110, only those PPOs 110 in their category, or a subset of PPOs 110 representing a particular condition. For example, a printer supplier might request that all printer PPOs 110 for Hewlett Packard printers be sent to them.

Detailed Description Text (72):

In an embodiment in which PPOs 110 are being transmitted to the seller, it is important to note that there are a number of hardware options for seller interface 300. Suitable seller interfaces 300 include fax machines, PDAs with wireless connections, and beepers or pagers. For example, a car dealer could instruct central controller 200 to beep him whenever PPO 110 appeared for his particular make of car, providing details of PPO 110 over the beeper network, or informing the seller to log on to central controller 200 for further details.

Detailed Description Text (73):
FIG. 7 illustrates the process by which a potential seller selects PPO 110. At step 700 the potential seller logs onto central controller 200 using modem 350 of seller interface 300. At step 710 the potential seller selects an appropriate category. For example, a large office supply chain may have just experienced the cancellation of a very large shipment to a major corporation and might search in the office supply category in the hopes of finding a PPO 110 requesting similar goods. At step 720, the potential seller browses the list of available PPOs 110 (i.e. those with a status of `active`). PPOs 110 may be listed with minimal details, with additional information available only if the potential seller is interested in bidding on PPOs 110. A potential seller wanting more information about PPO 100 may request additional data at step 730. In one embodiment, each PPO 110 is hyperlinked to a separate web page that provides complete details of the order. The potential seller clicks on PPO 110 and is immediately transferred to the page with additional detail. This detail might include the itemized list of required items and any additional conditions that may be imposed on the purchase. In another embodiment, PPO 110 is electronically transmitted directly to the seller, via EDI, electronic mail, fax, telephone, beeper, etc.

Detailed Description Text (74):
FIG. 8 illustrates the process by which PPO 110 is bid on by a seller. At step 800, the potential seller selects PPO 110, which he would like to bid on, developing seller bid 115, which represents his bid. At step 810 central controller 200 receives seller response 115 from the potential seller. Central controller 200 then time-stamps seller response 115 and authenticates the identity of the seller, as well as verifying his probable capacity to deliver the goods. The time-stamp allows central controller 200 to determine the first bid to be received. In the case of tying bids the deal will be done with the first bid received. If two seller responses 115 are received within a few seconds of each other, the time-stamp allows central controller 200 to decide which was received first. Alternatively, the time-stamp may be appended to seller response 115 at the time it is transmitted from seller interface 300 using clock 335 of seller interface 300. Authentication of the seller's identity involves central controller 200 extracting the seller ID from seller response 115 and looking up the seller's identity in seller database 260. Information in seller database 260 then provides an indication of the seller's ability to deliver the goods. Before a seller can bid on PPO 100 for an office supplies, for example, central controller 200 must authenticate that the seller is an office supply company. If necessary central controller 200 may verify that the seller can provide the specific goods requested. Rather than just verifying that the seller is an office supply company, central controller 200 may verify that it also specializes in gold plated pens.

Detailed Description Text (75):
Central controller 200 then verifies the status of PPO 110 at step 830, determining whether or not the status of PPO 110 is "active" at step 840. If PPO 110 is currently "active" a unique tracking number is added to seller bid 115 at step 860. Central controller 200 then stores seller bid 115 in seller response database 270 at step 870. If the status of PPO 110 is not "active" at step 840, central controller 200 refuses seller bid 115 and transmitted back to the potential seller at step 850.

Detailed Description Text (76):
Referring now to FIG. 9, there is illustrated a procedure for the selecting the optimal bid for each PPO 110. At step 900, central controller 200 searches PPO database 267 to see if there are any PPOs 110 with a pooling date that is equal to the current date. If there are none this process is complete and stop at step 905. At step 910, the central controller finds the next (first) PPO 110 with a current pool date. At step 920, the central controller searches the seller bidding database 270 to see if there are any other valid bids on this PPO 110. If there are none, first check to see if there is a current best bid on this PPO. If there are no other valid bids and no current best bid, return to step 900 and start again. If there are bids, find the next (first) bid. At step 940, this bid is compared to the current best bid. If it is not better than the current best bid, return to step 920 and check to see if there are any other valid bids. If it is better than the current best bid, store it as the best bid and return to

step 920.

Detailed Description Text (79):
FIG. 10 illustrates the exchange of goods between buyer and seller. At step 1000, the seller receives a purchase notification. As mentioned above this could occur in a variety of mechanisms including PDAs, beepers etc. At step 1010, the seller transfers the specified goods to the buyer. This transfer could involve the delivery of physical goods as well as digital goods. Physical goods might include cars, jewelry, computer equipment, etc. digital goods might include documents, computer software, tickets, access codes, etc. A computer manufacturer, for example, might ship a computer to the buyer. At step 1020, the buyer examines the delivered goods to see if they meet all conditions and terms of FPO 100. A buyer purchasing a computer, for example, would verify that the computer had all the correct peripherals and associated software. At step 1040 if the goods do not meet the buyer's conditions as described in FPO 100 the buyer contacts an arbiter at central controller 200 for dispute resolution. This process is described in more detail In the dispute resolution embodiment described later. If the goods meet the conditions, payment is transferred to the seller at step 1050. At step 1060 the transaction is complete.

Detailed Description Text (81):
There are many methods by which the providers of the system (the intermediary) could derive a revenue stream. In one embodiment, a flat fee is charged for every FPO 100 submitted. There could also be flat fees that would cover any number of FPOs 100 over a given period of time, allowing buyers to subscribe to the service much as they would subscribe to a newspaper. In another embodiment central controller 200 calculates a commission to add to the best bid on PPO 110 before it is allocated to each individual FPO 100. In another embodiment, advertisers pay to have messages listed along with PPOs 110 or on the catalog selection pages, supplementing the costs of operating the system. Alternatively, the method and apparatus of the present invention may be employed without a payment feature.

Detailed Description Text (82):
FIG. 11 illustrates a protocol in which central controller 200 establishes buyer account 297. At step 1100, the buyer selects his preferred method of payment. Preferred methods might include credit cards, personal checks, electronic funds transfer, digital money, etc. At step 1110 the buyer transmits payment data corresponding to his preferred method of payment to central controller 200. As indicated by box 1115, such payment data might include credit card number or bank account number. These payment methods are meant to be merely illustrative, however, as there are many equivalent payment methods commonly known in the art, which may also be used. If the buyer wants to pay by credit card, for example, payment data would include his credit card account number, expiration date, name of issuing institution, and credit limit. It should be noted that for some international credit card transactions the beginning date of the credit card need to be used in conjunction with the expiration date to determine if the card is valid. For electronic funds transfer, payment data includes the name of the buyer's bank and his account number. At step 1120, the central controller 200 stores payment data and payment preferences in payment database 285. At step 1130, central controller 200 establishes buyer account 297, which either stores money transferred by the buyer or serves as a pointer to an account of the buyer outside the system. For buyers using credit cards, for example, buyer account 297 contains the credit card number, expiration date and name of issuing institution. Buyers could also transfer money to central controller 200 to be stored in buyer account 297, which would operate like a conventional checking account. Central controller 200 could send a check to the seller written on buyer account 297. Alternatively, central controller 200 could electronically move the funds directly from buyer account 297 to the intermediary account 296. As noted above there are numerous payment permutations for paying the intermediary and the seller. At step 1140, central controller 200 contacts the bank or card issuer to confirm that funds are available. A buyer is thus unable to use a credit card with no credit available to establish buyer account 297.

Detailed Description Text (83):
The above protocols may be similarly applied to sellers, allowing for the creation of seller account 298. The primary difference being that seller account 298 is primarily used for deposits, with money flowing from seller to buyer in the case of deposit returns or refunds when the buyer does not find the received goods acceptable. Verification of funds available is therefore not as important for sellers.

Detailed Description Text (84):

In the on-line embodiment, central controller 200 performs processing the buyer's credit card. Central controller 200 looks up the credit card number of the buyer in payment database 285. This credit card number is transmitted to payment processor 230. Payment processor 230 contacts the credit card clearinghouse to get an authorization number. The billable amount appears on the credit card statement of the buyer in his monthly statement. The clearinghouse posts this amount to intermediary account 296. Central controller 200 updates payment database 285 to indicate that payment has been made by the buyer.

Detailed Description Text (85):
Another on-line embodiment describes a protocol in which central controller 200 transmits the buyer's credit card information to the seller for processing. Central controller 200 could also arrange for payment to be made directly to the seller account 298 from buyer account 297. Although only two methods are described herein, those skilled in the art will know that there are of course many payment protocols under which payment may be transferred from buyer to intermediary, to seller.

Detailed Description Text (86):
Another method of payment involves procedures using digital cash. Central controller 200 looks up the buyer's electronic delivery address in payment database 215. This address is transmitted to payment processor 230, with the digital cash being downloaded from the buyer. Central controller 200 updates payment database 285 to indicate that payment has been made by the buyer. This address might be an electronic mail address if the digital cash is to he transferred by electronic mail, or it could be an Internet protocol address capable of accepting an on-line transfer of digital cash. This electronic delivery address is sent to payment processor 230. The digital cash is downloaded to intermediary account 298 or directly to the seller account 298 or directly to seller. Central controller 200 then updates payment database 285 to indicate that payment has been made. Using these digital cash protocols, it is possible for the buyer to include payment along with FPO 100 in electronic form.

Detailed Description Text (87):
In yet another embodiment, the procedure of using digital cash could include the use of smart cards. An example of such a device is the SmartPortDT manufactured by Tritheim Technologies, Inc. The SmartPortDT is an intelligent desktop smart card reader/writer designed for electronic commerce, network and Internet security and software copy protection. The SmartPortDT is fully Compliant with ISO 7816 T=0, T=1, T=14, PC/SC and Mondex standards. These cards are currently being used by several electronic payment systems, such as Mondex and Visa cash. The practice of using digital cash protocols to effect payment is well known in the art and need not be described here in detail. For reference, one of ordinary skill in the art may refer to Daniel C. Lynch and Leslie Lundquist, Digital Money, John Wiley & Sons, 1996: or Peter Wayner, Digital Cash: Commerce on the Net, Academic Press, 1996.

Detailed Description Text (89):
Escrow account 299 allows payment to be delayed until the seller completes delivery of the goods, while at the same time ensuring that the buyer will in fact make payment. Central controller 200 establishes escrow account 299 as a temporary holding account. When the seller is awarded PPO 100 funds are transferred from buyer account 297 to escrow account 299. Only after the buyer has received the goods are funds transferred from escrow account 299 to intermediary account 296. The buyer may transmit a digitally signed release message to central controller 200, authorizing the release of the escrowed funds to the seller.

Detailed Description Text (90):
In another embodiment, the buyer makes a partial payment when PPO 110 is awarded, and then completes payment when the goods ore received. The fraction of the bid price of PPO 110 to be paid upon award of the best bid is stored in payment database 285 when FPO 100 is created. Central controller releases this portion of the funds to the seller, and then releases the remaining portion after goods have been delivered. The partial payment made upon award of the best bid may be non-refundable. This would allow a travel agent, for example, to sell vacation package reservations to a group of people with the proviso that the reservations that are cancelable on two days notice, with cancellations within the two day period resulting in forfeiture of deposit.

Detailed Description Text (93):
A buyer may use a telephone, for example, to generate FPO 100. The buyer calls central controller 200 and is connected with an agent. The buyer provides the items of FPO 100 such as

category, description of goods, quantity, pool date, etc. The buyer also provides his buyer ID, password, or private key so that central controller 200 can authenticate his identity. The agent puts this data into digital form by typing it into a terminal. The agent then provides the buyer with the ceiling price for each item. Once the buyer accepts the ceiling price, the agent then adds legal language to form FPO 100. FPO 100 is then transmitted to central controller 200 where it is converted into PPO 110 as described in the on-line embodiment.

Detailed Description Text (94):
In an alternative embodiment, the buyer calls central controller 200 and is connected with a conventional Interactive Voice Response Unit (IVRU) which allows the buyer to enter some or all of the terms of FPO 100 without the assistance of a live agent. The buyer initially selects from a menu of categories with the touch-tone keys of his phone. The specific items can also be selected in the same manner. The central controller can then announce the ceiling price for each item and the buyer can then use his touch-tone keys to select the quantity required. This information can then be used to generate PPOs 110.

Detailed Description Text (95):
Potential sellers may also use a telephone to browse and bid on PPOs 110. The potential seller calls central controller 200 and selects a category. Central controller 200 then converts the list of each PPO 110 into audio format reading the entire list to the potential seller. At any time during the reading of PPOs 110, the potential seller may press a combination of keys on his telephone to select PPO 110 for bidding. The central controller could then convert the itemized list of items on the PPO 110 to audio format. on completion, the seller enters seller ID number and is authenticated by central controller 200 prior to his bidding of PPO 110. He could then use the keys on his phone to enter his bid. Potential sellers could also enter parameters before having the list of PPOs 100 read to them. A computer manufacturer, for example, might request that all computer PPOs 110 for more than eight hundred units be read, skipping any PPO 110 with a lower count.

Detailed Description Text (96):
Buyers may also communicate with an agent at central controller 200 through faxes or postal mail. The agent receives the message and proceeds to digitize it and form FPO 100 and PPO 110 as described above.

Detailed Description Text (97):
In the previous embodiments, authentication of the buyer and seller involves checking the attached ID or name and comparing it with those stored in seller database 260 and buyer database 255. Although this procedure works well in a low security environment, it can be significantly improved through the use of cryptographic protocols. These protocols not only enhance the ability to authenticate the sender of message but also serve to verify the integrity of the message itself, proving that it has not been altered during transmission. A small computer manufacturer, for example, could be prevented from, bidding on PPOs 110 requiring delivery of thousands of computers, as their identity would not be authenticated for a transaction requiring the performance of a larger manufacturer. Encryption can also prevent eavesdroppers from learning the contents of the message. A competing manufacturer, for example, could be prevented from reading any intercepted seller bid 115 generated by another competitor. Such techniques shall be referred to generally as cryptographic assurance methods and will include the use of both symmetric ad asymmetric keys as well as digital signatures and hash algorithms.

Detailed Description Text (99):
FIG. 12 describes a symmetric key embodiment in which the seller and central controller 200 share a key. Thus both encryption and decryption of seller bid 115 are performed with the same key. This encryption may be implemented with an algorithm such as DES (U.S. Government standard, specified in FIPS 46, published in November 1976), or with any of several algorithms known in the art such as Triple DES, IDEA, Blowfish, RC4, RC2, CAST, etc. The seller encrypts seller bid 115 with his assigned symmetric key at step 1200 using cryptographic processor 310 of seller Interface 300. The key may be stored in message database 370 or otherwise noted or memorized by the seller. The encrypted seller bid 115 is then transmitted to cryptographic processor 210 of central controller 200 at step 1210. Cryptographic processor 210 extracts the seller ID from seller bid 115 at step 1220 and looks up the symmetric key of the seller in cryptographic key database 290 at step 1230, decrypting seller bid 115 with this key at step 1240. Cryptographic key database 290 contains algorithms and keys for encrypting, decrypting and/or authenticating messages. At step 1250, if the resulting message is intelligible, then

the same key must have encrypted it. Authenticating that the seller must have indeed been the author of seller bid 115.

Detailed Description Text (100):
This procedure makes it significantly more difficult for an unauthorized seller to represent himself as a legitimate seller. Without cryptographic procedures, an unauthorized seller who obtained a sample seller bid 115 from a legitimate seller would be able to extract the seller ID and then attach this ID number to unauthorized seller bids 115. When seller bid 115 has been encrypted with a symmetric key, however, an unauthorized seller obtaining a sample seller bid 115 only discovers the seller's ID number, not the symmetric key. Without this key, the unauthorized seller cannot create a seller bid 115 that will not be discovered by central controller 200, since he cannot encrypt his message in the same way that the authorized seller could. The symmetric key protocol also ensures that seller bid 115 has not been tampered with during transmission, since alteration of the message requires knowledge of the symmetric key. An encrypted seller bid 115 also provides the seller with more anonymity.

Detailed Description Text (101):
Referring now to FIG. 13, there is shown an asymmetric key protocol in which seller bid 115 is encrypted with a private key and decrypted with a public key. Two such algorithms for this procedure are RSA and DSA. At step 1300, the seller encrypts seller bid 115 with his private key using cryptographic processor 310, transmitting seller bid 115 to central controller 200 at step 1310. Cryptographic processor 210 extracts the seller ID at step 1320 and looks up the seller's associated public key in cryptographic key database 290 at step 1330, decrypting seller bid 115 with this public key at step 1340. As before, if seller bid 115 is intelligible then central controller 200 has authenticated the seller at step 1350. Again, unauthorized sellers obtaining seller bids 115 before central controller 200 received it are not able to undetectably alter it since they do not know the private key of the seller. Unauthorized sellers would, however, be able to read the message. If they managed to obtain the public key of the seller. Message secrecy is obtained if the seller encrypts seller bids 115 with his public key requiring the attacker to know the seller's private key to view seller bid 115.

Detailed Description Text (102):
FIG. 14 shows a cryptographic technique using digital signatures to provide authentication and message integrity. One such algorithm is DSA (Digital Signature Algorithm) uses U.S. Government standard specified in FIPS PUB 186. As in the asymmetric protocol described above each seller has an associated public and private key. The seller signs seller bid 115 with his private key at step 1400 with cryptographic processor 310 and transmits it to central controller 200 at step 1410. Central controller cryptographic processor 210 extracts she seller ID at step 1420 and looks up the seller's public key at step 1430 verifying the signature using seller bid 115 and the public key of the seller at step 1440. If seller bid 115 is intelligible, then central controller 200 accepts seller bid 115 as authentic at step 1450.

Detailed Description Text (103):
Referring now to FIG. 15, there is described a cryptographic technique using message authentication codes for verifying the authenticity and integrity of seller bid 115. In the hash protocol of the present invention, the seller and central controller 200 share a symmetric key, which the seller includes in a hash of seller bid 115, at step 1500. In the hash protocol, a one-way function is applied to the digital representation of seller bid 115, generating a code that acts much like the fingerprint of seller bid 115. Any of the MD algorithms, such as RIPEMD-160, MD5, SHA-1, MDC-2, MDC-4 and the like may be applied In this application. After transmitting seller bid 115 to central controller 200 at step 1510, cryptographic processor 210 extracts seller ID from seller bid 115 at step 1520. Then cryptographic processor 210 looks up the seller's symmetric key at step 1530 and hashes seller bid 115 with this symmetric key at step 1540, comparing the resulting hash value with the hash value attached to seller bid 115. If the values match at step 1550, the integrity of seller bid 115 is verified along with the authenticity of the seller.

Detailed Description Text (104):
Although cryptographic techniques can provide greater confidence in the authenticity of seller bids 110, they are useless if the seller's cryptographic keys are compromised. An attacker obtaining the symmetric key of another seller is indistinguishable from that seller in the eyes of central controller 200. There is no way to know whether the seller was the true author of seller bid 115, or an attacker with he right cryptographic keys. One way to solve this problem (known as undetected substitution) is to use biometric devices such as a fingerprint reader,

voice recognition system, retinal scanner and the like. These devices incorporate a physical attribute of the seller into seller bid 115, which is then compared with the value stored in seller database 260 at central controller 200. In the present invention, such devices attach to seller interface 300.

Detailed Description Text (105):
Fingerprint verification, for example, may be executed in several forms. (a) before the creation of seller bid 115, (b) during the generation of seller bid 115 in response to prompts from central controller 200, (c) at some predetermined or random times, or (d) continuously by incorporating the scanning lens into seller interface 300 such that the seller is required to maintain his finger on the scanning lens at all times for continuous verification while seller bid 115 is generated.

Detailed Description Text (106):
An example of such an identification device is the FingerCheck FC200 available from Startek, a Taiwanese company. The FC200 is readily adaptable to any PC via an interface card and is about the size of a computer mouse. The fingerprint verifier utilizes an optical scanning lens. The seller place his finger on the lens and the resulting image is scanned, digitized, and the data compressed and stored in memory. Typically, a 256-byte file is all that is required. Each live-scan fingerprint is compared against the previously enrolled/stored template, stored in data storage device 360. If the prints do not match cryptographic algorithms executed by cryptographic processor 335 may prevent the seller from generating a bid 115.

Detailed Description Text (107):
In a voice verification embodiment, the seller's voice is used to verify his identity, This embodiment has the advantage of not requiring the use of any specialized hardware since it can be implemented over a standard phone connection. The seller's identity is verified at central computer 200. The process of obtaining a voiceprint and subsequently using it to verify a person's identity is well known in the art and therefore need not he described in detail herein. One of ordinary skill in the art may refer to SpeakEZ, Inc. for voice identification/verification technology. Conventional speaker identification software samples the seller's voice. This sample is stored at central controller 200 in seller database 260. Each time the seller wants to transmit seller response 110 to central controller 200, he is required to call central controller 200 and speak into the phone at the prompt for a voice sample. If this sample matches that stored in seller database 260, the seller is provided a password which is incorporated into the digital signature appended to seller bid 115. Any seller bid 115 received without appropriate voice match password is not accepted. The voiceprint may also be stored in a database within data storage device 360 of seller interface 300, to verify seller's identity locally prior to allowing seller bid 115 to be created.

Detailed Description Text (108):
Another method of authentication and identification is the use of smart cards 365 attached to sellers interface 300. An example of such a device is the SmartPortDT manufactured by Tritheim Technologies, Inc. The SmartPortDT is an intelligent desktop smart card reader/writer designed for electronic commerce, network and Internet security and software copy protection. The SmartPortDT is fully Compliant with ISO 7816 T=0, T=1, T=14, PC/SC and Mondex standards. In this embodiment, the intermediary provides each potential seller with a smart card. Embedded on the smart card is the seller ID and a second private key for the seller, which would remain unknown to the seller. In this protocol unauthorized sellers would have to have knowledge of the seller's keys (symmetric, asymmetric or hash function) and would have to be in possession of the seller's smart card. This technique could also be augmented with biometric devices.

Detailed Description Text (109):
In another embodiment, sellers could be provided with a hardware device used for authentication. These devices are usually called tokens. Two common tokens are made by Security Dynamics and by Axent. The Security Dynamics SecurID card has a window on the front, which displays a cryptographically generated random number, which changes once a minute. The matching authentication server, central controller 200, can duplicate the computation to verify the number. The seller simply copies the number from the card along with his seller ID in sellers bid 115. The Axent Defender card is a small calculator device with a key pad and a display. In operation, the central controller 200 sends the seller a challenge code, which is entered into the card along with the sellers ID. The seller transmits the response code to central controller 200. Central controller 200 executes the same computation and compares the result.

Detailed Description Text (110):
Although the above cryptographic and biometric protocols describe the authentication and validation of seller bids 115, they may be equally applied to the authentication and validation of FPO 100, purchase confirmation 120, or any at message or communication between buyers, sellers, and central controller 200.

Detailed Description Text (111):
Currently there are two encryption protocols that are standard components of Internet browsers. These are available in such browsers as Netscape Navigator and Microsoft Internet Explorer. These protocols are the Secure Socket Layer (SSL) and the Secure Electronic Transaction (SET). In one embodiment, these techniques could also be used to achieve some of the cryptographic requirements mentioned above.

Detailed Description Text (112):
As mentioned previously, the present invention provides for the anonymity of both buyers and sellers. Such anonymity is accomplished by eliminating all references to names of the individuals for all transactions. The process of creating PPO 110 from FPO 100 ensures that the seller need not be notified of the buyers' identities. Also buyers are prevented from seeing other buyers FPO 100 and so their identities are kept from other members of the pool. In this embodiment, the payment protocol of buyers paying the intermediary and then the intermediary paying the seller ensure complete anonymity for both buyer and seller. This is desirable if the buyer were an individual who did not want to be inundated with direct mail solicitations usually generated from the purchase of certain item.

Detailed Description Text (115):
Although using ID numbers can provide anonymity, both for buyers and sellers, there are a number of potential weaknesses. First, if the database of ID numbers stored in buyer database 255 or seller database 260, and the intermediary is compromised, anonymity is destroyed since the message sender can be looked up in buyer database 255 or seller database 260. To prevent this, the ID numbers are encrypted with the public key of central controller 200, so that even if it is stolen it is useless without the private key.

Detailed Description Text (117):
In one embodiment of the present invention, central controller 200 is separated into three distinct elements: operations server 160, certificate authority 165, and settlement server 170. Each server performs a distinct task in the process of managing FPO 100 and seller bids 115. This separation makes it more difficult for attackers to compromise the system, as they must defeat the security of three separate systems, instead of one. As indicated in FIG. 16, these servers work in conjunction with buyer interface 400 and seller interface 300. Operations server 160 has the task of posting FPOs 100, PPOs 110 and receiving buyers bids 115 and accepts all transactions previously authenticated by certificate authority 165. Certificate authority 165 authenticates the identity of buyers and sellers while settlement server 170 verifies the ability of buyers to pay and the ability of sellers to deliver on FPOs 100 and seller bids 115. In this embodiment, each server type may be distributed over a number of servers.

Detailed Description Text (119):
An example of such a system is the CertAuthority Solution manufactured by CertCo LLC. This system also comes with an optional temper evident hardware based private key that is easy to transport and store securely. An example of a settlement server is the Integrated Commerce Service manufactured by Open Market Inc. It provides back-office services necessary to run Web-based businesses. Services include on-line account statements, order-taking and credit card payment authorization, credit card settlement, automated sales tax calculations, digital receipt generation, account-based purchase tracking, and payment aggregation for low-priced services.

Detailed Description Text (120):
The practice of using certificate authorities and settlement servers is well known in the art and need not be described here in detail. For reference, one of ordinary skill in the art may refer to Winfield Treese and Lawrence Stewart, Designing Systems for Internet Commerce, Addison Wesley, 1998.

Detailed Description Text (124):
In a buyers auction embodiment, there is only a single buyer in the pool. Different from a standard auction in which the seller wishes to sell a particular item or service and seeks a

buyer who is willing to pay the most for that item, in a buyer's auction, the buyer is looking for a particular item or service and it is the sellers who bid to win the business. An example would be a buyer who wishes to reserve a limousine from JFK airport to the Waldorf Astoria hotel in New York City at 10am on a certain date. The buyer enters a FPO 100 for a limousine as stated above and would then post the PPO 110 for sellers to bid on. In the buyer auction embodiment, no pooling is performed on FPO 100, the sellers bid on providing the posted service. In this embodiment the central controller 200 may provide the buyer with a maximum price of the service or alternatively the buyer may post a reserve price i.e. a maximum price he is willing to pay for the item or service. The process for the creation of FPO 100, PPO 110 and the sellers bids are as described above for FIGS. 5 to 10.

Detailed Description Text (125):
In a forward price embodiment, instead of providing a ceiling price per item, the central controller 200 provides the buyer with a list of forward prices. The list is the price of the item for a given purchase date. If a buyer could wait for the manufacturer to produce the goods, he could get a cheaper price then a buyer who needed the item immediately. The buyer who needed the goods immediately would have to compensate a supplier for the added expense of keeping an inventory on hand. This concept is similar to just in time purchasing for large corporations, but now would be available to small corporations and individuals.

Detailed Description Text (126):
Not all transactions require the transfer of money from buyer to seller. In a barter transaction the distinction between buyer and seller disappears, resulting in a contract between a number of first parties and a second party. The first party creates FPO 100 and specifies the quantity of goods he is ordering and then specifies a list of equivalent goods he is willing to receive. He may also provide a measure to equate "worth" of each of the separate items. The central controller may give him an indication of the ceiling number of each of the alternatives he may receive. This information is then aggregated into PPO 100. The second party now bids on PPO by specifying how much of a particular alternative he is ordering. Once again the optimal bid is calculated and awarded to the corresponding seller. Instead of getting cash, the second party receives goods from the first party. An example of this would be several small countries each willing to order raw materials in exchange for the delivery of medical supplies.

Detailed Description Text (128):
Although the previous embodiments have described the delivery of goods from seller to buyer as the end of the process, there will inevitably be disputes arising from some transactions, requiring follow-up activity to resolve these disputes. The present invention can support dispute resolution in two ways.

Detailed Description Text (130):
Second, central controller 200 can support the arbitration process by providing an arbiter for each dispute. Such arbitration might be required when goods shipped from the seller do not correspond to the conditions of FPO 100 and PPO 110. A buyer requiring a 400 MHz Pentium II processor in his computer, for example, might seek damages against a seller who delivered a computer with a 350 MHz Pentium II processor. Instead of seeking damages, the buyer may seek replacement of the goods, such as another printer instead of the one that was malfunctioning. In arbitration involving computers, the buyer may submit a copy of the shipping documents to central controller 200 along with the tracking number of FPO 100, allowing the arbiter to establish whether or not to seller fulfilled the conditions of FPO 100 and PPO 110. Sellers may also initiate arbitration proceedings if they have shipped the goods and have not yet received payment from the intermediary.

Detailed Description Text (131):
In an alternative embodiment, transaction data can be sent to third party arbiters outside the system. Central controller 200 may send a copy of FPO 100, PPO 110, seller's bid 115 and purchase confirmation 120 to the arbiters. Cryptographic keys may also be provided to the arbiters if there are questions of authenticity or non-repudiation.

Detailed Description Text (154):
11) Mutual Fund Purchase

Detailed Description Text (155):
Many mutual funds offer large volume purchases the ability to buy the fund at NAV. By pooling

together, buyers may be able to achieve the same leverage as institutional buyers.

Current US Class (1):
705

CLAIMS:

1. A computer based method for facilitating a transaction between at least two buyers, an intermediate, and at least one seller, comprising:

receiving at the intermediate a forward purchase order for at least one item from at least two buyers, said intermediate having a central controller;

forwarding a purchase stipulation from the central controller to the at least two buyers responsive to the submitted forward purchase order;

upon receiving an acceptance of said purchase stipulation, aggregating said forward purchase order to orders of like kind in a pool to form a pooled purchase order;

making the pooled purchase order including conditions of said pool to at least one seller;

receiving a bid from at least one seller;

verifying said bid with conditions of said pool;

if conditions of said pool are satisfied, binding the seller to said intermediate and storing said bid in seller database;

selecting a best bid from said database to determine a selected seller; and

forwarding confirmations of sale to the at least two buyers and the selected seller.

5. The method of claim 1, wherein the purchase stipulation is a commission or cancellation fee defined by the central controller.

8. The method of claim 1, wherein the forward purchase order further comprises a quantity specifier, a pool date, and a buyer identification.

9. The method of claim 1, further including the steps of authenticating the identification of the buyer.

10. The method of claim 9, wherein said step of authenticating is performed by said central controller by authenticating the buyer's credit card with a credit card issuer.

12. The method of claim 7, wherein the step of authenticating the buyer's identification includes communication of cryptographic messages.

15. The method of claim 14, wherein the step of providing payment to the selected seller includes use of an automatic payment management system at the central controller.

16. The method of claim 14, wherein the step of providing payment includes establishing an escrow account associated with the buyer.

20. The method of claim 18, wherein the plurality of sellers are identified by comparing with seller identification stored in the central controller database.

21. The method of claim 19, wherein authentication of the sellers identification is performed by cryptographic means.

22. The method of claim 1, wherein said receiving and forwarding steps are performed over an electronic network.

30. The method of claim 12, further including the step of determining at the intermediate if there are sufficient funds in the buyer's credit card account.

31. The method of claim 1, wherein said steps of receiving and forwarding between the at least one buyer, the intermediary, and at least one seller is conducted over a telephone network.

32. A computer based method for facilitating a transaction between at least one buyer, an intermediate, and at least one seller, comprising:

receiving at the intermediate a forward purchase order for at least one item from at least one buyer, said intermediate having a central controller;

forwarding a prenegotiated price for said items from the central controller to the buyer responsive to the submitted forward purchase order;

upon receiving an acceptance of said prenegotiated price; and

forwarding confirmations of transaction to the buyer and the selected seller.

33. A device having computer readable code embodied therein for causing a computer to perform the method steps for facilitating a transaction between at least two buyers, an intermediate, and at least one seller, comprising:

receiving at the intermediate a forward purchase order for at least one item from at least two buyers, said intermediate having a central controller;

forwarding a purchase stipulation from the central controller to the at least two buyers responsive to the submitted forward purchase order;

upon receiving an acceptance of said purchase stipulation, aggregating said forward purchase order to orders of like kind in a pool to form a pooled purchase order;

making the pooled purchase order including conditions of said pool to at least one seller;

receiving a bid from at least one seller;

verifying said bid with conditions of said pool;

if conditions of said pool are satisfied, binding the seller to said intermediate and storing said bid in seller database;

selecting a best bid from said database to determine a selected seller; and

forwarding confirmations of sale to the at least two buyers and the selected seller.

34. A method for facilitating a transaction between a buyer, an intermediate, and at least one seller, comprising:

receiving at the intermediate a forward purchase order for a goods or service from the buyer, said forward purchase order having a reserve price, said intermediate having a central controller;

forwarding a purchase stipulation from the central controller to the buyer responsive to the submitted forward purchase order;

receiving an acceptance of said purchase stipulation;

posting at said central controller said forward purchase order;

receiving a bid from at least one seller;

verifying said bid with conditions of said forward purchase order;

if conditions of said forward purchase order are satisfied, store bid in seller database;

selecting a best bid from said database to determine a selected seller; and

forwarding confirmations of sale to the buyer and the selected seller.

Previous Doc Next Doc Go to Doc#

Generate Collection Print

L12: Entry 77 of 77 File: USPT Mar 2, 1982

US-PAT-NO: 4317957
DOCUMENT-IDENTIFIER: US 4317957 A
** See image for Certificate of Correction **

TITLE: System for authenticating users and devices in on-line transaction networks

DATE-ISSUED: March 2, 1982

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Sendrow; Marvin	Annandale	VA	22003	

APPL-NO: 06/ 129110 [PALM]
DATE FILED: March 10, 1980

INT-CL: [03] H04L 9/00

US-CL-ISSUED: 178/22.08; 340/825.34, 235/379, 235/382
US-CL-CURRENT: 705/71; 235/379, 235/382, 380/281, 380/45, 705/43, 705/72, 713/185, 902/2, 902/5

FIELD-OF-SEARCH: 178/22, 178/22.08, 178/22.09, 375/2, 235/379, 235/380, 235/382, 340/149A, 340/149R

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3956615	May 1976	Anderson et al.	235/379
☐	3985998	October 1976	Crafton	340/149A
☐	4025760	May 1977	Trenkamp	340/149A
☐	4123747	October 1978	Lancto et al.	178/22
☐	4214230	July 1980	Fak	178/22
☐	4223403	September 1980	Konheim	178/22
☐	4238854	December 1980	Ehrsam et al	375/2
☐	4259720	March 1981	Campbell	375/2

ART-UNIT: 222

PRIMARY-EXAMINER: Birmiel; Howard A.

ATTY-AGENT-FIRM: Whitham; C. Lamont Ferguson, Jr.; Gerald J. Baker; Joseph J.

ABSTRACT:

A method for efficiently protecting transactions and providing authentication of users and devices in on-line systems that transfer funds electronically, dispense cash, or provide a good or permit a service to be utilized is provided. The transaction may be initiated by a magnetic-striped plastic card at an attended or unattended terminal (10, 11, 12) and requires the entry of a preassigned Personal Identification Number through a keyboard (20). The Personal Identification Number is encrypted (23) more than once at the terminal and other means are used in order to prevent the utilization of certain tapped-line data. The data required to validate and authorize the transaction is transmitted securely to a centralized computer (14) which accesses from its stored data base (15) the data that is required to decrypt and validate the transaction, including the encrypted Personal Identification Number corresponding to the received transaction data. A secret Terminal Master Key must be maintained securely at each terminal and may differ at each terminal. A list of such Terminal Master Keys and other secret data must be securely maintained at the centralized computer. Means for multiple-encryptions and decryptions in a predetermined way must also be maintained at each terminal and at the centralized computer. Means (34) are provided for securely returning a response to the terminal at which the transaction was initiated to authorize or reject the requested transaction. These functions are accomplished in a way that permits efficient utilization of data communications lines and reduces or eliminate perpetration of fraud by any of various means.

17 Claims, 9 Drawing figures

Previous Doc Next Doc Go to Doc#

L12: Entry 77 of 77 File: USPT Mar 2, 1982

DOCUMENT-IDENTIFIER: US 4317957 A

** See image for Certificate of Correction **

TITLE: System for authenticating users and devices in on-line transaction networks

Abstract Text (1):

A method for efficiently protecting transactions and providing authentication of users and devices in on-line systems that transfer funds electronically, dispense cash, or provide a good or permit a service to be utilized is provided. The transaction may be initiated by a magnetic-striped plastic card at an attended or unattended terminal (10, 11, 12) and requires the entry of a preassigned Personal Identification Number through a keyboard (20). The Personal Identification Number is encrypted (23) more than once at the terminal and other means are used in order to prevent the utilization of certain tapped-line data. The data required to validate and authorize the transaction is transmitted securely to a centralized computer (14) which accesses from its stored data base (15) the data that is required to decrypt and validate the transaction, including the encrypted Personal Identification Number corresponding to the received transaction data. A secret Terminal Master Key must be maintained securely at each terminal and may differ at each terminal. A list of such Terminal Master Keys and other secret data must be securely maintained at the centralized computer. Means for multiple-encryptions and decryptions in a predetermined way must also be maintained at each terminal and at the centralized computer. Means (34) are provided for securely returning a response to the terminal at which the transaction was initiated to authorize or reject the requested transaction. These functions are accomplished in a way that permits efficient utilization of data communications lines and reduces or eliminate perpetration of fraud by any of various means.

Brief Summary Text (3):

This invention relates to the secure generation and transmission of Transaction Request Messages and Responses in on-line Electronic Funds Transfer and other types of networks consisting of remote terminals in communication with a central data base containing encrypted data used in the validation or authentication process or similar networks used to transfer funds and that provide for, in addition to transferring funds, dispensing cash, paying bills, making deposits, dispensing a good or permitting utilization of a service.

Brief Summary Text (5):

Both on-line and off-line computer networks and systems have been developed for executing user initiated or requested financial transactions for reasons of public convenience and economy. One example is a cash dispensing machine. Such a machine may be activated by use of an appropriately coded check or other negotiable instrument, or a plastic credit, debit or identification card, and dispenses the requested amount of cash if the request seems valid to the authenticating means in the cash dispensing device.

Brief Summary Text (6):

One type of on-line system stores account information in a central data base to which the remote terminals are connected by data communication lines. In response to submission of specified information from a remote terminal, such as account number, amount of sale or amount requested, merchant identification if a sale, and secret information related to the cardholder, the system searches the account files to obtain data that may indicate that the transaction should be approved or denied. Such information may include date of last use, amount of credit if a credit transaction, balance in account, whether a card has been lost, stolen or has expired. If the transaction is approved, the system adjusts the account information appropriately after the transaction is completed. As the art progressed, terminals with increased functions were provided that permitted more functions to be performed than dispensing cash or effecting a purchase. For instance, financial institutions, to reduce peak loads and to

extend their services during times of business closure, permit the transfer of funds between accounts, accept payments for utilities or for loan balances, accept deposits, and provide for advances to be charged to valid credit cards. These devices typically include a plastic card reading mechanism, a keyboard, a display, document entry and exit apertures and may be connected to a data base or operate as a stand-alone device. Due to the increased functions permitted, the exposure to fraud increased, so that secret numbers (Personal Identification Numbers) were issued to cardholders to reduce the exposure. The Personal Identification Number entered on the keyboard by the cardholder must either compare directly with the number encoded on the magnetic stripe of the plastic card or some correspondence, that may depend on encryption, must exist between the Personal Identification Number and the number encoded on the magnetic stripe. Otherwise, the transaction is not enabled on the presumption that the card was either lost or stolen. This method may be used by stand-alone devices or devices connected to a central data base.

Brief Summary Text (7):
The use of a Personal Identification Number improved the security of such systems but still left some means available for fraud and had other disadvantages. The problem of secure issue of Personal Identification Numbers arose. The use of on-line files with lists of Personal Identification Numbers may permit unauthorized access to the files by employes for purpose of obtaining what is supposed to be secret information. With such information, duplicate or counterfeit cards can easily be manufactured to perpetrate fraud. Several different approaches were taken to overcome the disadvantages. One approach, to avoid the use of on-line files and to overcome the supposed cost and complexity of on-line systems, was to try to improve the security of stand-alone use. As a result, special plastic cards with material laminated into the card, pasted onto the card, holes punched into or onto the card as a security measure, were devised, none of which was effective by itself.

Brief Summary Text (8):
Another approach was to encrypt the Personal Identification Number stored in the account records, which is effective, provided appropriate additional security measures are instituted. Encryption may not be effective with stand-alone devices because of access required by maintenance personnel and for replenishing the cash supply or other servicing, thereby exposing the encryption key to simple means of compromise. Encrypting only the secret information in the central account records is not effective since the secret information must also be entered at a remote terminal to initiate a transaction and be transmitted, usually by means of utility communication lines, to the centralized computer, thereby becoming subject to monitoring by person or persons unknown. The transmission therefore must also be encrypted, which is effective but may still permit someone who can break the code access to the list of correspondence between account information and Personal Indentification Numbers by monitoring these transmissions. An additional shortcoming is the generation, by a sophisticated penetrator, of spurious transactions to fraudulently transfer funds within data base accounts. As a result, the previous methods of validating the secret number at a centralized data processor provide protection against casual fraud but may not provide adequate protection against a penetrator having knowledge of, and perhaps, access to, current data processing equipment or systems. Alternatively, those methods that seem to provide an adequate level of security also seem quite costly due to the need for utilizing high-cost data communication lines for multiple transmissions for validation of each transaction and for transmission in a secure way of the required enciphering keys, rather than relying on a single Transaction Request Message, a single Response and an acknowledgement or some minimum number of transmissions per transactions.

Brief Summary Text (9):
There has evolved within the same time frame networks other than the proprietary networks that a single financial institution may deploy to service its customers. Financial Institutions may decide to share networks or to interchange transactions in order to provide better service. There are national networks developed by Bank Cards to service many financial institutions that may aggregate millions of accounts and millions of transactions per day. Although each transaction may be small, the aggregate dollar volume transferred per day is substantial. In addition, there are the semi-official clearing house systems and the networks used by Federal Financial Agencies to transfer billions of dollars of funds daily and that impact the financial structure of the country. The methods used by some of the large financial institution networks to provide security are so simplistic, they may easily be defeated by a knowledgeable person, as occasional newspaper headlines attest.

Brief Summary Text (10):
What has been lacking until now is a procedure, method or system that integrates the validation and authentication of the plastic card, cardholder, terminal or other device used to initiate transactions, render ineffective wiretap data, that does not require unencrypted Personal Identification Numbers to be processed, that efficiently uses costly data communication lines by minimizing transmissions and is adaptable to the requirements of different types of on-line networks.

Brief Summary Text (12):
A system in accordance with the present invention consists of a means for multiply-enciphering secret and other data in a predetermined way at a remote terminal or a computer connected by communication lines to a computer, said enciphering to provide authentication of the card, cardholder, terminal or other device, and to provide security against intrusion by wiretapping in a way that maximizes utilization of communication lines. The secret data may be entered on a keyboard by an authorized cardholder together with other data that may be required to complete the transaction. The secret and other data, and data internal to the remote terminal or computer, are multiply-enciphered in a predetermined way using a secret Terminal Master Key stored in the terminal or computer, initially to generate a Working Key that is used only to encipher the Transaction Request Message that is generated within the terminal or computer by suitable means. The Working Key is then additionally multiply-enciphered in a predetermined way using the secret Terminal Master Key to generate a Transmitted Key that is appended to the Transaction Request Message and transmitted by suitable means to the computer at the centralized account data base in a way that prevents intrusion by wire tapping. At the centralized computer, the account data base is searched to find enciphered and other data corresponding to the account of the authorized cardholder and the device from which the message was received, which data is used two ways. Part of the data is used to facilitate the multiple decipherments of the Transmitted Key in order to obtain the Working Key. Other parts of the data are used to validate and authenticate the transaction after it has been deciphered using the Working Key and the Working Key itself has been further multiply-deciphered and in a way that provides that the enciphered data is protected from access by employees of the financial institution such as programmers, systems analysts, operators and also protected from other sophisticated penetrators who may gain unauthorized access to the computer network or system. After the transaction has been validated, additional tests of an accounting nature may be performed by the central computer to determine whether the Transaction Request should be approved, tests depending upon data such as balance in account, date of last use, amount withdrawn and other data. An appropriate response is generated at the centralized computer by suitable means, which response is enciphered in the same Working Key used to encipher the Transaction Request Message. This Transaction Request Response is transmitted by suitable means to the terminal or computer from which the Transaction Request Message was received, where it is deciphered by suitable means using the Working Key that has been securely stored and the requested transaction is completed if approved, or an indication displayed that the transaction is not approved. After completion of the transaction, the terminal or computer may send an acknowledgement to the centralized computer indicating the type of transaction completed, as an added security measure, which acknowledgement may be enciphered using the same Working Key. After the centralized computer receives the acknowledgement, it updates the accounting data base and then the remote terminal or computer and the centralized computer destroy the Working Key securely by resetting the register or location in which the Working Key has been stored to prevent reuse or compromise.

Brief Summary Text (13):
Because the secret data and other data are used to generate the working key required to encipher each Transaction Request Message, each such Message will be enciphered using a different Working Key before being transmitted to the centralized computer, substantially enhancing the strength of the enciphering means and protecting the Terminal Master Key from compromise by statistical cryptanalysis. In the preferred embodiment, there is only 1 chance in 2 to the 56th power that the same Working Key would be generated twice.

Drawing Description Text (3):
FIG. 1 is a functional block diagram representation of a typical on-line financial network in which the present invention may be implemented.

Drawing Description Text (5):
FIG. 3 is a representation of one method of forming Security Parameter 1 at a terminal or computer to initiate the process of the present invention.

Drawing Description Text (6):
FIGS. 4, 5, 6 are alternative methods of forming Security Parameter 1 to suit the needs or characteristics of different types of financial, on-line networks.

Detailed Description Text (3):
Terminal: A device such as a Cash Dispenser, Automatic Teller Machine, Point-of-Sale device, or any of various types of computers that may be used to initiate a financial transaction.

Detailed Description Text (4):
Terminal Identification (TID): A designation of 8--8 binary digit numbers, letters or a mixture of numbers and letters that identifies a specific terminal and is embodied as an integral characteristic of the terminal.

Detailed Description Text (5):
Primary Account Number (PAN): A designation that identifies an account holder in an accounting data base.

Detailed Description Text (6):
Personal Identification Number (PIN): A variable number of digits, letters or a mixture of digits and letters known only to an authorized account holder and used in the initiation and validation of on-line financial transactions. In the preferred embodiment, at least 4 characters are used as the Personal Identification Number. The binary designation chosen for these and other parameters may be any of those commonly used in computer processing or data communications without affecting the scope of the invention.

Detailed Description Text (7):
Card anti-counterfeiting features (CS): A designation or identification for a magnetic-striped, plastic, size "A" card that cannot be changed without destroying the card.

Detailed Description Text (9):
Master Key (KMO if at a centralized computer, KMT if at a terminal): A key used primarily or solely to encrypt and decrypt other keys.

Detailed Description Text (10):
Master Key Variants (KM1 and KM2 if at a centralized computer, KMT1 and KMT2 if at a terminal): A Master Key with certain specified binary digits inverted to provide a defense against specific types of penetration by an intruder. In the 56 binary digit representation, KM1 and KMT1, called the first variants, are equal to the respective Master Keys with binary digits 2, 9, 16, 23, 30, 37, 44, 51, counting left to right, inverted. Then, KM2 and KMT2, called the second variants, are formed from the respective Master Keys by having binary digits 5, 12, 19, 26, 33, 40, 47, 54 inverted.

Detailed Description Text (11):
Working Key (WK): A key used to encrypt or decrypt a Transaction Request Message. In this invention, it differs for each transaction to provide an enhanced degree of security.

Detailed Description Text (12):
Transmitted Key: A key transmitted with a transaction and used to provide a defense against wire tap and used to facilitate decryption.

Detailed Description Text (17):
E[KMT] (Key) at terminal.

Detailed Description Text (20):
D[KMT] (Key) at a terminal.

Detailed Description Text (27):
Referring now to the drawings, and more particularly to FIGS. 1 and 2, the invention will be described in terms of a preferred embodiment. This embodiment comprises a network having cash dispensing machines, automatic teller machines or the like such as would be used by a bank or similar financial institution. It is to be expressly understood, however, that the invention has broad and general applications including, but not limited to, transferring funds, dispensing a good or permitting the utilization of a service.

Detailed Description Text (28):
A cardholder enters his magnetic striped size "A" plastic card into an attended or unattended financial terminal 10, 11, 12, enters his Personal Identification Number and amount requested or amount of transaction on a keyboard at 20. The terminal reads the magnetic stripe and extracts the Bank Identification Number, the Primary Account Number and adds the Terminal Identification at 21. The terminal generates the Transaction Request Message at 22 and uses the Primary Account Number, the Personal Identification Number, the card anti-counterfeiting feature number and the Time field to generate Security Parameter 1, which is used with the Terminal Identification and the Terminal Master Key within the encryption means to generate the Working Key at 23 in a manner to be explained with reference to FIGS. 7A to 7C. The Working Key is used to encrypt the Transaction Request Message at 24 already generated. The Working Key, the terminal Identification and the Terminal Master Key are used to generate the Transmitted Key at 25 in a manner to be explained with reference to FIGS. 7A to 7C. The Transmitted Key is appended to the Transaction Request Message in addition to transit, routing and other control information that may be required such as an Initialization Vector required to initialize the DES in some usages, and the complete message is transmitted to the centralized computer 14 at 26 by transmission means.

Detailed Description Text (29):
The centralized computer 14 obtains data, some of it encrypted, from the accounting data base 15 using the control information in the message header and other information and sends it all to the Security Module 13 at 27. The Security Module 13 uses the Terminal Identification, the Terminal Master Key and Transmitted Key within the encryption means to obtain the Working Key at 28 in a manner to be described with reference to FIGS. 7A to 7C. The Working Key is used within the Security Module 13 to decrypt the Transaction Request Message at 29. The Security Module 13 uses the Working Key, the Terminal Master Key and the Terminal Identification within the encryption means to obtain Security Parameter 1 in a manner to be explained with reference to FIGS. 7A to 7C in order to obtain access to the Personal Identification Number and card anti-counterfeiting feature number at 30. The Security Module 13 verifies that the Personal Identification Number and card anti-counterfeiting feature number that was generated from the data in the message is the same as those values contained in the accounting data base transferred from the centralized computer by any one of several means at 31, and notifies the centralized computer 14.

Detailed Description Text (30):
The centralized computer 14 executes the remainder of the approval process at 32, generates and transmits to the Security Module 13 the appropriate response at 33. The Security Module 13 encrypts the response using the Working Key at 34, after which the response is transmitted to the terminal 10, 11 or 12 by transmission means. The terminal decrypts the response using the Working Key at 35, provides the service requested at 36, generates an acknowledgement at 37, encrypts the acknowledgement using the Working Key at 38 and transmits it to the centralized computer 14. The centralized computer 14 sends the acknowledgement to the Security Module 13 at 39. The Security Module 13 decrypts the acknowledgement using the Working Key, notifies the centralized computer 14 and destroys the Working Key at 40. The centralized computer 14 updates the account base 15 at 41, the terminal 10, 11 or 12 updates and writes the magnetic stripe on the plastic card if required, destroys the Working Key at 42, completing the transaction at 43. With reference now to FIGS. 7A to 7C, the present invention may be implemented on a financial transaction or transfer network such as that represented in FIG. 1 that contains attended or unattended terminals 10, 11, 12 or a computer 16 with transmission and encryption means and associated Security Module 17 and data base 18 connected by data communication lines to a centralized computer with transmission means 14, encryption means 13, and with access to a centralized accounting data base 15, which may be any one of several media for storing, retrieving and changing data usually by magnetic or electromagnetic means. The accounting data stores information related to each account assigned to authorized account holders of the Financial Institution. The terminals or computer may be connected to the centralized computer by any of various means familiar to those skilled in the art. In order to initiate a transaction on such a network, an authorized cardholder enters his magnetic striped, size "A" plastic card into a card entry means at the terminal 50 as shown in FIG. 7A, the terminal determines whether the cardholder has been requested to enter his Personal Identification Number more than a fixed number of times at 51, in the preferred embodiment three times. If the cardholder has entered his Personal Identification Number three times, the terminal retains the card at 52, indicates that the cardholder must visit his Financial Institution at 53 and terminates the transaction at 54.

Detailed Description Text (31):
If the cardholder has not entered his Personal Identification Number three times, the terminal requests the cardholder to enter his Personal Identification Number on the keyboard at 55, which the cardholder does at 56, the terminal reads the magnetic stripe at 57, the terminal forms Security Parameter 1 at 58 by using part of the Primary Account Number, part of the Personal Identification Number, part of the card anti-counterfeiting number and part of the Time field as shown in FIG. 6 or alternatively as shown in FIGS. 3, 4, 5. The terminal requests the cardholder to enter the type of transaction and the amount at 59, which the cardholder does at 60, the terminal generates the Transaction Request Message at 61. The terminal generates a Secondary Key by decrypting the terminal identification using the Terminal Master Key at 62:

Detailed Description Text (32):
The terminal generates Security Parameter 2 using function Reencrypt from Master Key and operands Secondary Key and Security Parameter 1 at 63 as specified below:

Detailed Description Text (34):
The terminal generates Working Key using function Reencrypt from Master Key and operands Secondary Key and Security Parameter 2 at 64 as specified below:

Detailed Description Text (35):
The terminals encrypts the Transaction Request Message using the Working Key at 65, as specified below:

Detailed Description Text (36):
The terminal generates Security Parameter 3 using function Reencrypt to Master Key and operands Secondary Key and Working Key at 66 as specified below:

Detailed Description Text (38):
The terminal generates Transmitted Key using function Reencrypt to Master Key and operands Secondary Key and Security Parameter 3 at 67 as specified below:

Detailed Description Text (39):
The terminal appends the Transmitted Key to the Transaction Request Message in addition to other routing, transit and control information required in the message header at 68. The terminal encrypts the complete message including the header using a link encryption key at 69 and transmits it to the centralized computer at 70. The centralized computer sends the message to the Security Module at 71, the Security Module decrypts the message using the link encryption key at 72, the Security Module sends the routing, transit and control information to the centralized computer at 73, the centralized computer determines whether this is an "on-us" transaction or an interchange transaction at 80. If it is an interchange transaction, additional processing is required which will be described later.

Detailed Description Text (40):
If this is not an interchange transaction, the centralized computer obtains various data from the accounting data base for which it may use the Terminal Identification to obtain the Terminal Master Key (encrypted) as may be stored similar to Table 3 and sends all the data to the Security Module at 74.

Detailed Description Text (44):
The Security Module decrypts the Transaction Request Message using the Working Key at 77, as specified below:

Detailed Description Text (48):
The Security Module recovers part of the Primary Account Number, part of the Personal Identification Number, part of the card anti-counterfeiting number from Security Parameter 1 if FIG. 6 was originally used at the terminal 81 or whatever was used if alternative FIGS. 3, 4 or 5 were used. The Security Module recovers the remainder of the Primary Account Number from the decrypted Transaction Request Message and sends the complete number to the centralized computer at 82, the centralized computer retrieves the encrypted Personal Identification Number and the card anti-counterfeiting feature number from the accounting data base using the Primary Account Number at 83 as may be stored similar to Table 6.

Detailed Description Text (49):

The centralized computer sends the data to the Security Module to validate the transaction at 84, the Security Module compares the Personal Identification Number obtained from the Accounting Data Base after appropriate decryption with that generated from the Transaction Request Message and compares the two anti-counterfeiting numbers to validate the transaction at 85, 86. If the transaction does not appear valid, the Security Module indicates that the centralized computer should specify to the terminal a request that the cardholder re-enter his Personal Identification Number at 87 shown in FIG. 7B which the centralized computer does at 88, returning to processing at 51 shown in FIG. 7A.

Detailed Description Text (50):
If the transaction appears valid, the Security Module notifies the centralized computer at 89, the centralized computer executes the remainder of the approval procedure at 90, generates an approval or disapproval response and sends it to the Security Module at 91. The Security Module encrypts the response using the Working Key and returns it to the centralized computer at 92, the centralized computer transmits the response to the terminal at 93. The terminal decrypts the response using the Working Key at 94, the terminal provides the service if approved or displays a message if disapproved at 95, the terminal generates an acknowledgement at 96, the terminal encrypts the acknowledgement using the Working Key and transmits it to the centralized computer at 97. The centralized computer sends the acknowledgement to the Security Module at 98, the Security Module decrypts the acknowledgement and notifies the centralized computer at 99, the centralized computer updates the account data base and notifies the Security Module and the Terminal at 100, the Security Module destroys the Working Key at 101, the Terminal updates the magnetic stripe if required and returns the card to the cardholder at 103, the Terminal destroys the Working Key at 104, and the transaction is complete at 102.

Detailed Description Text (51):
If the transaction is an interchange transaction, the centralized computer (acquirer) uses the Bank Identification Number or similar designation to obtain the encrypted Site Master Interchange Key, the encrypted Passwork, the Computer Identification (acquirer) as may be stored similar to Table 7 in addition to the data normally retrieved and sends it all to the Security Module at 105. The Security Module uses the Site Master Interchange Key in place of the Terminal Master Key, uses the Password in place of the Personal Identification Number, uses the Computer Identification in place of the Terminal Identification, uses the Bank Identification Number in place of the Primary Account Number and uses part of the Time field to generate an Interchange Working Key as was done at 62 to 64 in FIG. 7A, at 106. The Security Module encrypts the Terminal Identification and the Terminal Master Key (after it has first been decrypted), using the Interchange Working Key, generates an Interchange Transmitted Key as was done at 66, 67 in FIG. 7A, appends the Interchange Transmitted Key, the header and control information to the Transaction Request Message and encrypts it using a link encryption key at 107, the Security Module sends the transaction to the acquirer centralized computer at 108. The acquirer centralized computer transmits the transaction to the issuer centralized computer at 109, the issuer centralized computer sends the message to the issuer Security Module at 110 shown in FIG. 7C.

Detailed Description Text (52):
The Security Module decrypts the transaction using the Link Encryption Key, sends the header and control information to the issuer Centralized Computer at 111, the issuer Centralized Computer uses the information to retrieve the encrypted Site Master Interchange Key, the encrypted Password and the Computer Identification and sends it to the Security Module at 112, the Security Module uses the same procedure as was used at 75, 76 in FIG. 7A, to recover the Interchange Working Key at 113 and uses the same procedure as was used at 78, 79, 81 in FIG. 7A, to recover the Password which is validated at 113. The Security Module uses the Interchange Working Key to recover the Terminal Identification and Terminal Master Key by decryption at 114. The remainder of the procedure to recover the Personal Identification Number, to validate and approve the transaction and generate a response is the same as was used at 75 to 79, 81 to 91 in FIGS. 7A and 7B at 115. The issuer Security Module encrypts the response that will go to the terminal using the Working Key at 116, encrypts the response to acknowledgement to go to the acquirer centralized computer using the Interchange Working Key and sends it to the issuer Centralized Computer at 117. The issuer Centralized Computer transmits the response to the acquirer centralized computer at 118, the acquirer Centralized Computer sends the response to the Security Module at 119, the Security Module decrypts the response using the Interchange Working Key and sends to the acquirer Centralized Computer the part of the response that is to be transmitted to the terminal and the Centralized Computer updates its in-process file at 121. The terminal follows the same procedures as in 94 to 97 in FIG. 7B, at 122. The acquirer

Centralized Computer relays the acknowledgement to the issuer Centralized Computer at 123, the issuer Centralized Computer follows the same procedure as in 98 to 101 in FIG. 7B, at 124. The acquirer Centralized Computer updates the in-process file, relays notification to terminal at 128, the acquirer Security Module destroys the Working Key at 125, the terminal updates the magnetic stripe if required, returns the card to the cardholder at 129, destroys the Working Key at 126, and the transaction is complete at 127.

Detailed Description Text (53):
Considering FIG. 1, "Computer with transmission means," 14, may consist of an IBM 370/148 Central Processing Unit (CPU), 3410 Tape units, 1403 Printer, 3705 Communications Controller, Bell 201C Data Sets. The Data Base may be accommodated on one or more IBM 3330 Disks, 15. The Cash Dispenser, 10, or ATM, 11, may consist of IBM 3614's that may include an Intel 8080 microprocessor and Motorola MGD8080DSM Data Security Module. The Security Module, 13, or 17, may consist of an Intel 8080 microprocessor and a Motorola MGD8080DSM Data Security Module. The other computer shown in FIG. 1, 16, may consist of a Burroughs 7766 CPU, 9495 Tape units, 9373 Disk units (18), Documation 1500 printer, Burroughs 7350 Communications Controller, TA1201 Data Sets, and RT 4000 Cash Dispensers or ATM's deployed similar to those shown communicating with the computer system, 14. In either case, the terminals indicated in 12 may be IBM 3604, 3612, or 3610 or Burroughs TU700, TC700. The communication lines may be 300 to 1200 baud, synchronous or asynchronous.

Detailed Description Text (55):
The set of programs which follow implements the procedure previously described using an Intel 8080 Microprocessor with an attached Motorola MGD8080DSM Data Security Module. These devices are one possible implementation of the "Security Module" 13, FIG. 1. The programs are "stand-alone" for test purposes. That is, there has been no attempt to integrate these programs into the programs required for an operating, on-line network. However, any of several operating network programs can easily be modified to use the programs shown here by placing the proper set of "CALL's" at appropriate points of the operating program since the programs included here are comprehensive in that they implement all the functions required to mechanize the security procedure described in earlier sections of this application. Although this test program uses the DES in Electronic Code Book Mode exclusively, the DES may be used in Cipher Feedback or Block Chaining mode at appropriate places without limiting or changing the scope of the invention.

Detailed Description Text (57):
1. A main routine to generate either WK and TK given SP1, TID and KMT or generate WK and SP1 given TK, TID and KMT. The same program may be used at a terminal or at a HPC, with the proper parameter supplied to the program. The difference is that at the HPC, the terminal Master Key, KMT, is encrypted using the Host Master Key, KMO, while at the terminal, KMT is not encrypted. In addition, SP1 is a starting parameter at the terminal and TK is a starting parameter at the HPC. These differences are accommodated within the programs.

Detailed Description Text (59):
3. A testing program that simulates the operations that would normally take place at a terminal and those that would normally take place at a HPC. The procedure at the terminal is to use the remainder of the programs to generate TK and WK after SP1, KMT and TID are supplied. Then, a Transaction Request test message is enciphered using WK, and transmission of the message and TK to the HPC is simulated.

Detailed Description Text (60):
At the HPC, generation of WK and SP1 is accomplished given TK, KMT, TID, using the same set of programs, and the test message is deciphered using WK. Both versions of the test message, and both versions of SP1 and WK are compared for equality. If they are equal, the HPC program initiates the encipherment of a response message and simulates transmission to the terminal.

Detailed Description Text (61):
The terminal program initiates decipherment of the response message using WK and compares it to the original message. If the fields compared are equal, the test program halts at a normal stop. If any fields compared are not equal, the program stops at an error halt.

Detailed Description Text (75):
This routine first deciphers the Working Key using the Master Key and immediately loads the deciphered key into the Active Key Register where it can be used for enciphering or deciphering

data. Ahtough not used by the testing program, this routine will be required in any operational network and, so, is included.

Detailed Description Text (82):
16. START, Routine to Debug, Simulates the Terminal and HPC.

Detailed Description Text (83):
This routine is used only for testing the remainder of the set of programs by simulating calls to the Main Routine as if from a Terminal and a HPC, and comparing the results. It uses a set of constants and parameters which may also be deleted after testing is complete. Once initiated at START, it runs to completion at FINIS. If there are errors, various error halts are included within each of the routines.

Detailed Description Text (92):
In the preferred example, an authorized holder of a size "A" magnetic-striped plastic card, which may be a Debit, Credit or Identification Card, would enter the card in a cash dispensing machine or automatic teller machine, enter his secret Personal Identification Number on a keyboard, and indicate the type and amount of transaction by pushing appropriate buttons provided for that purpose. The device would read the data on the magnetic stripe, such as account number and other data, and would also have available internally by electronic means a suitable Terminal Identification Code, a time clock and a secret Terminal Master Key. The device would generate, by appropriate means, a Transaction Request Message whose content would be determined by the type of transaction, amount requested and other data. In addition, the device would use part of the secret Personal Identification Number, part of the account number, part of the "Time" field, and part of a card anti-counterfeiting field if there is one, to generate a parameter that would be one input into a suitable encryption means. Additional inputs in a specified order or sequence would be the Terminal Master Key and the Terminal Identification. Multiple encryptions in a predetermined way would result in the generation of a Working Key, which would temporarily replace the Terminal Master Key within the encryption means and be used to encipher the Transaction Request Message and other data that may be required. The Working Key is then multiply-enciphered in a predetermined way using the Terminal Master Key and Terminal Identification to generate the Transmitted Key which is appended to the enciphered Transaction Request Message together with any additional data required to process the transaction such as routing, transit and other control information, and/or an Initialization Vector that may be required to initialize or synchronize the deciphering means. A link encryption key may then be used to encipher all of the data to be transmitted to protect the network against "traffic analysis" intrusion by wire tap. The Transaction Request Message and header and control data are transmitted to the centralized computer, which may require intermediate receivers and transmitters (nodes) in a large network. At some nodes, decipherment using the link encryption key may be required, with subsequent encipherment using a different link encryption key appropriate for the next segment of the transmission. At the centralized computer, the message is first deciphered using the last-used link encryption key. Then the other data in the header or control part of the message and data available in the centralized data base, some of which may be enciphered, are used to multiply-decipher the Transmitted Key, preferably in a physically and electronically separate and secure device sometimes called a Network Security Controller (NSC) or a Security Module (SM), which process of decipherment results in generation of the Working Key that was used to encipher the Transaction Request Message at the terminal. The Working Key is used to decipher the Transaction Request Message and is then additionally multiply-decrypted to obtain the parameter that was used at the terminal to initiate the process. Since that parameter contains part of the secret Personal Identification Number, part of the account number and part of the card anti-counterfeiting features, if there is one, the validity of the transaction can be determined by comparison of the fields in the message with the corresponding fields of data obtained from the centralized data base, for which comparison additional encipherments and/or decipherments may be required. Specifically, the account number in the message may be used to obtain the corresponding secret Personal Identification Number and the card anti-counterfeiting number if there is one from the centralized data base which are compared with the corresponding partial fields that were, by implication, included in the message at the terminal. In the preferred embodiment, the secret Personal Identification Number is not otherwise directly included in the Transaction Request Message, it is independently generated at the centralized computer by decipherments in a predetermined way, so that a penetrator somehow obtaining a deciphered message still does not have access to any data that will permit compromise of that account or any other account or aspect of system operation. The card anti-counterfeiting number, if there is one, also need not be included in the Transaction Request Message provided it is used at the terminal to generate

the parameter that enters into the first encipherment. Since the multiple encipherments at the terminal also include the Terminal Identification and the secret Terminal Master Key, it is not possible for a penetrator to substitute a spurious terminal in the network for the purpose of initiating fraudulent transactions to transfer funds. In the preferred embodiment, part of the "Time" field is included in the parameter that is enciphered at the terminal, to insure that each Transaction Request Message is enciphered using a different Working Key.

Detailed Description Text (93):
At the centralized computer, after the Transaction Request Message is validated, as described, additional processing may be required to determine if the transaction should be approved by determining if the account balance is adequate, if the transaction requested is valid for the specific account, if the plastic card used to initiate the transaction is not out-of-date, lost or stolen and by other processing that may be required. In the present example, the transaction is approved, the centralized computer generates an appropriate response which is enciphered within the NSC or SM using the same Working Key and transmitted to the terminal that initiated the transaction, from node to node, as may be required, and with link encryption as may be required. The terminal deciphers the response and provides the requested service by dispensing the amount of cash requested. The terminal generates an acknowledgement that may include the type of service provided and amount, encrypts it using the same Working Key that was used for the Transaction Request Message, and transmits it to the centralized computer. After the centralized computer receives the acknowledgement, it changes the accounting data base to reflect the results of the transaction, then the terminal and the centralized computer destroy the Working Key securely by resetting the register or location in which the Working Key was stored, and the transaction is complete. The transaction need not be to dispense cash, it may be to transfer funds, accept a deposit, make an advance to a valid credit card or against a reserve account or may be other types of transactions that may be provided by the Financial Institution for its depositors.

Detailed Description Text (94):
A secret Terminal Master Key is required to be securely stored at each terminal, computer or other device that may initiate a message. In the preferred embodiment, the Terminal Master Key is never transmitted in any form but distributed by armed guard and entered under dual control into the encipherment means at each terminal, computer or other device, or other similar means are used that provides a similar level of security. Other systems that use encipherment also require manual entry of at least one secret key for proper operation. However, all other systems require more than 1 additional key be also entered or received at each terminal, some of which may be transmitted enciphered and are then deciphered in the terminal before use. In at least one system, the enciphering key that was used at the centralized computer to encipher all the secret Personal Identification Numbers, Key A, must be entered into each terminal in the network, which may number hundreds or more, thereby increasing the possibility of compromise. The Key A is distributed as Key A.sup.1 and manipulated internally in the terminal to form Key A, to reduce the possibility of compromise; nonetheless, such wide distribution still represents an exposure. In addition, a communications key is required at each terminal. In my invention, only one encryption key is required at each terminal, the Terminal Master Key or equivalent, thereby eliminating the exposure of the enciphering key that was used to encipher all the secret Personal Identification Numbers in the account data base. Furthermore, instead of only one key, Key A, being used to encipher all the secret Personal Identification Numbers in an account data base, multiple keys may be so used, reducing the intrinsic value of each such key considering bribery, coercion or blackmail, and facilitating plastic card reissue due to a change of equipment, change of technology, compromise of one or more enciphering keys, due to elapsed time, or for other reasons. In addition, using one key, Key A, may be adequate in a proprietary network, but does not facilitate sharing, or interchange of transactions between Financial Institutions. My invention provides for sharing and interchange.

Detailed Description Text (95):
In some networks, computer-to-computer messages are required for administrative purposes. My invention provides for such messages provided there is an analogue for the secret Personal Identification Number, such as a "Password," and analogues for the Terminal Master Key and for the Terminal Identification, as already described.

Detailed Description Text (96):
Yet other systems require that a terminal that is to communicate with a centralized computer must first send a message to a Network Security Controller (NSC) validating itself and requesting a Working Key or Communications Key. The NSC generates 2 copies of one key and

transmits one enciphered copy to the terminal and one enciphered copy to the centralized computer. The terminal deciphers the Working Key, uses it to encipher the message and transmits it to the centralized computer, where it may be deciphered. Multiple transmissions are required for each transaction in that system, decreasing effective utilization of costly data communications lines. My invention does not require the additional transmissions since authentication of the terminal and generation of the Working Key are integral to the operation of the system.

Detailed Description Text (97):
Because the method of using the Terminal Master Key in my invention protects it from exposure or compromise by cryptanalysis, it may be used for an extended period if not otherwise compromised. As a result, it is possible to use this invention in networks in which it would be difficult or impossible to permit changing a set of Master Keys on a frequent basis due to inaccessibility. One such network is one in which a communications satellite is used as a switching center. For example, a small number of transmitters may each have a need to transmit data to a large number of receivers in a way that does not permit other transmitters or some of the receivers to obtain access to the data transmitted. It would be an inefficient use of communications to require each transmitter or the satellite to maintain a separate enciphering key for each receiver and to separately encipher and process multiple copies of the same message, each originally enciphered using a different key. It is more efficient to permit the transmitter to encipher only one copy of a message and supply a list of recipients to the satellite, thereby permitting the satellite to decipher the message, and then to separately generate a Working Key to encipher one copy for each receiver using a different Master Key or set of Master Keys for each Working Key. The Master Keys could be combined 2, 3, 4 . . . (n-1) at a time by "exclusive or" to minimize the storage requirements, especially if there are a large number of receivers. The same methods as already described can be used provided each transmitter and receiver has a secret password, an Identification and a secret Master Key, and a means for encryption and decryption.

Detailed Description Text (98):
In the preferred embodiment described, the National Bureau of Standards Data Encryption Standard was used to clarify the description and explanation of the invention, which standard may be used in Electronic Code Book Mode, Cipher Feed Back Mode or Block Chaining Mode. Those skilled in the art will recognize that other cryptographic means or systems which require or permit a secret encryption key are as suitable, and that the use of 56 binary digit or 64 binary digit enciphering keys, and 64 binary digit blocks of plain text and cipher text are for illustrative purposes only and do not limit the scope of the invention. The method described can as well be implemented in software using a large scale computer, a minicomputer or a microcomputer, or in hardware using a large scale integrated circuit device designed and manufactured for the purpose or by other electronic devices. Instead of a "Time" field indicated previously, a currency counter, a transaction serial number or any other parameter that changes with each transaction can be used without changing or limiting the scope of the invention.

Detailed Description Text (99):
Although not a preferred embodiment, another variation in operation is feasible in some networks. In some networks it may be possible to include the PAN and TID as a header in the link encrypted part of the message. The PAN can be used at the centralized computer to retrieve the encrypted PIN from the data base after the Security Module decrypts the header using the last-used link encryption key. The Security Module decrypts the PIN and uses the PAN and the PIN to form SP1 and, by the method already described, generates the WK using the TID, KMT and its variants. The Security Module then decrypts the Transaction Request Message and may verify the PIN if it was encrypted with the Transaction Request Message. Alternatively, if the message decrypts properly using the WK, the correct PIN was used to initiate the transaction at the terminal by implication. If all this is done, it is not necessary to generate or transmit TK.

Detailed Description Text (100):
Although a particular embodiment of a system for authenticating users and devices in on-line transaction networks in accordance with the invention has been described for the purpose of illustrating the manner in which the invention may be used to advantage, it will be appreciated that the invention is not limited thereto. Accordingly, any modification, variation or equivalent arrangement within the scope of the accompanying claims should be considered to be within the scope of the invention.

Detailed Description Paragraph Equation (4):
E[WK](Transactions Request Message). (4)

Detailed Description Paragraph Equation (9):
D[WK](Transaction Request Message). (9)

Detailed Description Paragraph Table (3):
TABLE 3 TERMINAL MASTER TERMINAL IDENTIFICATION KEY (ENCRYPTED) TID 1 KMT 1 TID 2 KMT 2 TID 3 KMT 3 TID 4 KMT 4 0 0 0 0 0 0 TID n KMT n 0 0 0 0 0 0

Detailed Description Paragraph Table (6):
TABLE 6 PRIMARY PERSONAL ACCOUNT INDENTIFICATION CARD NUMBER NUMBER (ENCRYPTED) SIGNATURE PAN 1 PIN 1 CS 1 PAN 2 PIN 2 CS 2 PAN 3 PIN 3 CS 3 0 0 0 0 0 0 0 0 0 0 PAN n PIN n CS n 0 0 0 0 0 0 0 0 0 0

Detailed Description Paragraph Table (7):
TABLE 7 BANK COM- IDEN- SITE MASTER PUTER TIFICA- INTERCHANGE IDEN- TION KEY PASSWORD TIFICA- NUMBER (ENCRYPTED) (ENCRYPTED) TION BIN 1 SMIK 1 PW 1 CID 1 BIN 2 SMIK 2 PW 2 CID 2 BIN 3 SMIK 3 PW 3 CID 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 BIN n SMIK n PW n CID n 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Detailed Description Paragraph Table (8):
LIST OF ERROR HALTS
Label Comes at Routine From Halt Name (Label) Reason
MHLT1 MROUT MERR1 Parameter supplied neither 4 or 5 MHLT2 MROUT MERR2 Parameter supplied neither 4 or 5 MHLT3 MROUT MERR3 Parameter supplied neither 4 or 5 MWKHT1 MWKLD MWER1 DSM Status = Busy MWKHT2 MWKLD MWER2 DSM Parity Error MWKHT3 MWKLD MWER3 DSM Timed Out EDCP4 EDCPR EDER1 DSM Status = Busy EDCP5 EDCPR EDER2 DSM Parity Error EDCP6 EDCPR EDER3 DSM Timed Out MVE3 MOVE7 MVER1 DSM Parity Error MVE4 MOVE7 MVER2 DSM Timed Out WKL2 WKLOD WKER2 DSM Parity Error WLK3 WKLOD WKER3 DSM Timed Out WKL4 WKLOD WKER1 DSM Status = Busy CMPR3 COMPR CMPR2 The 2 fields being compared are not equal DBUG4 START DBER1 DSM Parity Error DBUG5 START DBER2 DSM timed out or not ready
NAME/LABEL OP CODE OPERAND COMMENTS ;
MAIN ROUTINE, CAN BE USED AT ; TERMINAL OR AT HOST PRO- ; CESSING CENTER (HPC). IF ; USED AT TERMINAL, WK & TK ; ARE GENERATED GIVEN SP1, TID, ; AND KMT. ALL INTERMEDIATE ; VALUES ARE GENERATED. WK ; HAS ODD PARITY AFTER COMPLE- ; TION OF THE ROUTINE. AFTER ; COMPLETION, THE OPERATING ; PROGRAM MUST REQUEST ENCI- ; PHERMENT OF THE TRANSAC- ; TION REQUEST MESSAGE USING ; WK BY MAKING 2 CALLS, ONE ; TO LOAD WK INTO ACTIVE REG. ; & ONE TO ENCIPHER N-8 BYTE ; GROUPS, APPEND TK AND TRANS ; MIT THE TRANSACTION RE- ; QUEST MESSAGE (TRM) TO THE ; HPC. WK IS SAVED IN ORDER ; TO DECIPHER RESONSE MESSAGE ; RECEIVED FROM THE HPC. ; REQUIRES MVI A, 5H (ENCIPH.) ; ; IF USED AT HOST PROCESSING ; CENTER (HPC), WK & SP1 ARE ; GENERATED GIVEN TK, TID & ; KMT, ALL REQUIRED INTER ; MEDIATE VALUES ARE GENER- ; ATED. WK HAS ODD RARITY. ; AFTER COMPLETION OF ROUTINE ; THE OPERATING PROGRAM MUST ; REQUEST DECIPHERMENT OF THE ; TRM USING WK BY MAKING 2 ; CALLS, ONE TO LOAD WK INTO ; ACTIVE REGISTER & ONE TO ; DECIPHER N-8 BYTE GROUPS ; VALIDATE THE PIN, ETC. IN ; SP1 TO AUTHENTICATE THE ; TRANSACTION, PREPARE A RE- ; SPONSE, USE CALLS TO ENCI- ; PHER RESPONSE USING WK, AND ; TRANSMIT RESPONSE TO THE ; TERMINAL. REQUIRES ; MVI A, 4H (DECIPHER). ; IN ADDITION, IN H & L REG. ; MUST BE THE ADDRESS OF THE ; FIRST OF A LIST OF 5 ; ADDRESSES AS FOLLOWS- ; 1. ADDR. OF SP1 LOCATION. IF ; AT TERMINAL OR INTO ; WHICH SP1 PLACED IF AT ; HPC ; 2. ADDR. OF TID LOCATION ; 3. ADDR. OF KMT LOCATION ; (KMT ENCIPHERED USING ; KMO IF AT HPC) ; 4. ADDR. OF 8-BYTE AREA ; INTO WHICH WK WILL BE ; PLACED ; 5. ADDR. OF 8-BYTE AREA ; INTO WHICH TK WILL BE ; PLACED IF AT TERMINAL ; OR ADDR. OF TK LOC. ; IF AT HPC. ; ; MVI A,5H IF TERMINAL OR ; MVI A,4H IF HPC ; LXI H, ADDRESS ; CALL MROUT ; NAME SENDRO MROUT: PUSH PSW PUSH B PUSH D STA MRPAR ; STORE EN/DE PAR ; AMETER LXI B, 2H ; CONSTANT TO B ; FOR ADDR. MODIF- ; ICATION SHLD IADSP1 ; STORE INDIR. SP1 DAD B ; INCR. ADDR. SHLD IADTID ; STORE INDIR. TID DAD B ; INCR. ADDR. SHLD IADKMT ; STORE INDIR. KMT DAD B ; INCR. ADDR. SHLD IADWK ; STORE INDIR. WK DAD B ; INCR. ADDR. SHLD IADTK STORE INDIR. TK LDA MRPAR ; LOAD EN/DE PARAM. CPI 5H ; COMPARE- IF TERM. JZ MRT1 ; IF TERMINAL, SKIP ; DECIPHERING KMT CPI 4H ; COMPARE IF HPC MERR1: JNZ MHLT1 ; JUMP TO ERROR ; HALT-NOT HPC MVI A, 3H ; PARAMETER TO LHLD LXI H, KMO ; LOAD MASTER KEY ; AS ACTIVE KEY CALL MWKLD ; CALL ROUTINE LHLD IADKMT ; INDIR. KMT ADDR ; TO H REG. SHLD $ + 1 ; STORE IN INSTR. LHLD OOH ; KMT ADDR TO H MVI

A, 4H ; PARAM. TO A LXI D, KMT ; LOCATION INTO ; WHICH KMT WILL ; BE PUT AFTER IT ; IS DECIPHERED ; USING KMO CALL EDCPR ; DECIPHER KMT LXI H, KMT ; KMT (DECIPHERED) ; ADDRESS TO H CALL MKODD ; MAKE ODD PARITY MRT1: MVI A,01000001B ; VARIANT 1 PARAM ; TO A REG. LXI D, KMT1 ; KMT1 ADDR TO D LXI H, KMT ; KMT ADDR TO H CALL GNMKV ; MAKE VARIANT 1 MVI A,00001001B ; VARIANT 2 PARAM LXI D, KMT2 ; KMT2 ADDR TO D LXI H, KMT ; KMT ADDR TO H CALL GNMKV ; MAKE VARIANT 2 LHLD IADKMT ; INDIR KMT ADDR ; TO H REG SHLD $ + 1 ; STORE IN INSTR. LHLD OOH ; KMT ADDR TO H MVI A, 3H ; PARAM. TO A CALL MWKLD ; LOAD KMT AS ; ACTIVE KEY LHLD IADTID ; INDIR TID ADDR ; TO H REG SHLD $ + 1 ; STORE IN INSTR. LHLD OOH ; TID ADDR TO H LXI D, SK ; ADDR SK TO H MVI A, 4H ; DECIPHER PARAM ; TO A REG. CALL EDCPR ; GENERATE SK = ; D/KMT/(TID) LXI H, KMT1 ; KMT1 ADDR TO A MVI A, 3H ; PARAM TO H CALL MWKLD ; LOAD KMT1 AS ; ACTIVE KEY MVI A, 4H ; DECIPH. PAR. A LXI H, SK ; SK ADDR TO H LXI D, DT1SK ; ADDR TO D CALL EDCPR ; GENERATE ; D/KMT1/(SK) LXI H, DT1SK ; ADDR TO H CALL MKODD ; MAKE ODD PARITY MVI A, 3H ; PARAM TO A LXI H, KMT2 ; KMT2 ADDR TO H CALL MWKLD ; LOAD KMT2 AS ; ACTIVE KEY MVI A, 4H ; DECIPHER PARAM ; TO A REG LXI H, SK ; ADDR SK TO H LXI D, DT2SK ; ADDR TO D CALL EDCPR ; GENERATE ; D/KMT2/(SK) LXI H, DT2SK ; ADDR TO H CALL MKODD ; MAKE ODD PARITY LDA MRPAR ; LOAD EN/DE PAR. CPI 4H ; COMPARE IF HPC JZ MRT2 ; IF HPC, JUMP TO ;OTHER ROUTINE CPI 5H ; COMPARE IF ; TERMINAL MERR2: JNZ MHLT2 ; JUMP TO ERROR ; HALT-NOT TERM. MVI B, 8H ; COUNT TO B LXI D, TEMP1 ; TO ADDR TO D LXI H, DT1SK ; FROM ADDR TO H CALL MOVEN ; MOVE 8 BYTES, MVI B, 8H ; COUNT TO B LXI D, TEMP2 ; TO ADDR TO D LXI H, DT2SK ; FROM ADDR TO H CALL MOVEN ; DT2SK TO TEMP2 LHLD IADSP1 ; INDIR SP1 ADDR ; TO H REG SHLD $ + 1 ; STORE IN INSTR. LHLD OOH ; SP1 ADD TO H MVI B, 8H ; COUNT TO B LXI D, TEMP3 ; TO ADDR TO D CALL MOVEN ; SP1 TO TEMP3 JMP MRT3 ; JUMP TO CONTINUE ; ROUTINE ; ; SUBROUTINE- IF HPC, SIMILAR ; TO PREVIOUS ROUTINE ; MTR2: MVI B, 8H ; COUNT TO B LXI D, TEMP1 ; TO ADDR TO D LXI H, DT2SK ; FROM ADDR TO H CALL MOVEN ; DT2SK TO TEMP1 MVI B, 8H ; COUNT TO B LXI D, TEMP2 ; TO ADDR TO D LXI H, DT1SK ; FROM ADDR TO H CALL MOVEN ; DT1SK TO TEMP2 LHLD IADTK ; INDIR TK ADDR ; TO H REG. SHLD $ + 1 ; STORE IN INSTR. LHLD OOH ; TK ADDR TO H MVI B, 8H ; COUNT TO B LXI D, TEMP3 ; TO ADDR TO D CALL MOVEN ; TK TO TEMP3 ; END OF SUBROUT. ; CONTINUE REST OF PROGRAM MRT3: MVI A, 3H ; SET KMT ACTIVE ; PARAMETER LXI H, KMT ; ADDR TO H CALL MWKLD ; CALL ROUTINE MVI A, 4H ; DECIPH. PAR. TO A LXI H, TEMP3 ; DATA TO BE

Detailed Description Paragraph Table (9):

; DECIPHERED LXI D, TEMP4 ; ADDR OF RESULT CALL EDCPR ; GENERATE ; D/KMT/(SP1) (E) ; OR D/KMT/(TK) (D) MVI A, 3H ; SET KEY ACTIVE ; PARAMETER LXI H, TEMP 1 ; ADDR TO H REG ; D/KMT1/(SK) (E) ; OR D/KMT2/(SK) (D) CALL MWKLD ; LOAD INTO ACTIVE ; REGISTER MVI A, 5H ; ENCIPHER PARAM. ; TO A REG. LXI H, TEMP4 ; DATA TO BE ENC- ; IPHERED LXI D, SP2 ; SP2 IF TERM., ; SP3 IF HPC CALL EDCPR ; GENERATE SP2 OR ; SP3 (D) MVI A, 3H ; SET KEY ACTIVE ; PARAMETER LXI H, KMT ; KMT ADDR TO H CALL MWKLD ; SET KMT AS ; ACTIVE KEY MVI A, 4H ; DECIPHER PARAM. ; TO A REG. LXI H, SP2 ; ADDR OF SP2 (E) ; OR SP3 (D) TO H LXI D, TEMP4 ; ADDR. OF RESULT CALL EDCPR ; GENERATE EITHER ; D/KMT/(SP2) (E) ; D/KMT/(SP3) (D) MVI A, 3H ; SET KEY ACTIVE ; PARAMETER LXI H, TEMP1 ; SET EITHER ; D/KMT1/(SK) (E) OR ; D/K MT2/(SK) (D) ; ACTIVE CALL MWKLD ; SET KEY ACTIVE MVI A, 5H ; ENCIPH. PARAM TO A LXI H, TEMP4 ; ADDR. OF EITHER ; D/KMT/(SP2) OR ; D/KMT/(SP3) LXI D, TWK ; RESULT ADDR TO D CALL EDCPR ; GENERATE WK LXI H, TWK ; WK ADDR TO H CALL MKODD ; MAKE WK ODD PARITY MVI A, 3H ; SET KEY ACTIVE ; PARAMETER LXI H, TEMP2 ; SET ACTIVE EITHER ; D/KMT2/(SK) (E) ; D/KMT1/(SK) (D) CALL MWKLD ; SET KEY ACTIVE MVI A, 4H ; DECIPH PAR. TO A LXI H, TWK ; WK ADDR TO H LXI D, TEMP4 ; RESULT ADDR TO D CALL EDCPR ; GENERATE EITHER ; D/D/KMT2/(SK)/ ; (WK) OR ; D/D/KMT1/(SK)/ ; (WK) LXI H, KMT ; KMT ADDRESS TO H MVI A, 3H ; SET KEY ACTIVE ; PARAMETER CALL MWKLD ; SET KMT ACTIVE MVI A, 5H ; ENCIPH PAR. TO A LXI H, TEMP4 ; ADDR. OF EITHER ; D/D/KMT2/(SK)/ ; (WK) OR ; D/D/KMT1/(SK) ; (WK) LXI D, SP3 ; RESULT ADDR TO D CALL EDCPR ; GENERATE SP3 (E) ; OR SP2 (D) MVI A, 3H ; SET ACTIVE PAR TO A LXI H, TEMP2 ; ADDR OR EITHER ; D/KMT2/(SK) (E) OR ; D/KMT1/(SK) (D) CALL MWKLD ; SET KEY ACTIVE MVI A, 4H ; DECIPH PARAM TO A LXI H, SP3 ; ADDRESS OF EITHER ; SP3 (E) OR SP2 (D) LXI D, TEMP4 ; RESLT ADDR TO D CALL EDCPR ; GENERATE EITHER ; D/D/KMT2/(SK)/(SP3) ; D/D/KMT1/(SK)/(SP2) MVI A, 3H ; SET KEY ACTIVE PAR. LXI H, KMT ; KMT ADDR TO H CALL MWKLD ; SET KMT ACTIVE MVI A, 5H ; ENCIPH PAR TO A LXI H, TEMP4 ; ADDR OF EITHER ; D/D/KMT2/(SK)/(SP3) ; D/D/KMT1/(SK)/(SP2) LXI D, TTK ; RESULT ADDR TO D CALL EDCPR ; GENERATE EITHER ; TK OR SP1 LHLD IADWK ; INDIR WK ADDR H SHLD $ + 1 ; STORE IN INSTR. LHLD OOH ; DIRECT WK ADDR H XCHG ; MOVE H TO D LXI H, TWK ; WK ADDR TO H MVI B, 8H ; COUNT TO B CALL MOVEN ; MOVE WK LDA MRPAR ; EN/DE PARAM TO A CPI 4H ; COMPARE IF HPC JZ MRT4 ; IF HPC, JUMP TO ; OTHER ROUTINE CPI 5H ; COMPARE IF TERM MERR3: JNZ MHLT3 ; JUMP TO ERROR ; HALT NOT TERM. LHLD IADTK ; INDIR TK ADDR H SHLD $ + 1 ; STORE IN INSTR LHLD OOH ; DIR. TK ADDR H XCHG ; MOVE H TO D LXI H, TTK ; ADD OF TK TO H MVI B, 8H ; COUNT TO B CALL MOVEN ; MOVE TK TO DTK JMP MRT5 ; JUMP TO CONT. ; IF HPC, TRANSFER SP1 ; MRT4: LHLD IADSP1 ; INDIR SP1 ADDR ; TO H SHLD $ + 1 ; STORE IN INSTR. LHLD OOH ; DIR. SP1 ADR. H XCHG ; MOVE H TO D LXI H, TTK ; ADDR OF SP1 TO ; H REG. MVI B, 8H ; COUNT TO B CALL MOVEN ; MOVE SP1 MRT5: POP D POP B POP PSW RET ; RETURN MHLT1: HLT ; FROM MERR1, NOT ; 4 OR 5, NOT ; TERMINAL OR HPC MHLT2: HLT ; FROM MERR2 NOT ; 4 OR 5, NOT HPC ; OR TERMINAL MHLT3: HLT ; FROM MERR3, NOT ; HPC OR TERM, ; NOT 4 OR 5 ; MASTER OR

WORKING KEY LOAD ; ROUTINE NO DECIPHER ; CALLING SEQUENCE ; MVI A, PARAMETER ; LXI H, MASKAD MASTER KEY ; CALL MWKLD ADDRESS OR ; WORKING KEY ; ADDRESS ; PARAM = 2H FOR MASTER KEY ; = 3H FOR WORKING KEY ; TO BE ACTIVE KEY ; MWKLD: PUSH PSW PUSH B PUSH D MVI B,OH ; CLEAR B REG MOV C, A ; MOVE PARAM TO C XCHG ; EXCHANGE D, H LHLD BPARAM ; LOAD BPARAM IN H DAD B ; ADD PARAM TO H SHLD MWK2 + 1 ; STORE RESULT IN ; INSTRUCTION XCHG ; RESTORE H & L IN BPARAM + REDST ; READ STATUS ORA A ; SET FLAGS MWER1: JNZ MWKHT1 ; GO TO HALT MVI B, 8 ; COUNT TO B REG MWK1: MOV A, M ; LOAD NTH CHAR MWK2: OUT OH ; OUTPUT NTH CHAR INX H ; INCR. FROM ADDR DCR B ; DECR. COUNT JNZ MWK1 ; LOOP MVI A, 50 ; COUNT 50 TO A MWK3: DCR A ; DECR. A REG JNZ MWK3 ; LOOP-PROG DELAY IN BPARAM + REDST ; CHECK STATUS ORA A ; SET POP D ; END ROUTINE POP B ; HOUSEKEEPING POP PSW ; RET ; RETURN MWKHT1: HLT ; BUSY HALT MWKHT2: HLT ; PARITY ERROR HLT MWKHT3: HLT ; TIME OUT HALT ; ROUTINE TO ENCIPHER OR ; DECIPHER N GROUPS OF 8 ; BYTES, N NO MORE THAN 254D. ; ANY NUMBER OF BYTES THAT ; ARE AN INTEGRAL MULTIPLE OF ; 8 BYTES MAY BE PROCESSED ; TO A MAXIMUM OF 2032D. ; PARAMETER IN A REG ; = 5H FOR ENCIPHER ; = 4H FOR DECIPHER ; B REG = NUMBER OF 8 BYTE GROUPS ; D & E REG. CONTAINS ADDRESS ; OF RESULTS ; H & L REG. CONTAINS ADDRESS ; OF DATA TO BE ENCIPHERED ; OR DECIPHERED ; IF ENCIPHER, H = PLAIN TEXT ; IF DECIPHER, H = CIPHER TEXT ; MVI A, PARAMETER ; MVI B, N ; LXI H, FROM ; LXI D, TO ; CALL NGEDR NGEDR: PUSH PSW STA NGPAR ; STORE PARAM MOV A, B ; N TRANSF. TO A STA NGRPS ; STORE N SHLD NFROM ; STORE FROM ADD. XCHG ; SHLD NTOAD ; STORE TO ADD. XCHG ; RESTORE ADI OOH ; SET FLAGS JZ NGOUT ; N = 0, COMPLETE LDA NGPAR ; LOAD PARAM, A NGD1: CALL EDCPR ; CALL 8 BYTE EN/ ; DE/CIPHER ROUT. LDA NGRPS ; N TO A REG DCR A ; DECR. N STA NGRPS ; STORE N - 1 JZ NGOUT ; IF ZERO, DONE LHLD NTOAD ; TO ADR. TO H LXI B, 0008H ; LOAD NO. 8, B & C DAD B ; ADD 8 TO `TO` ; ADDRESS SHLD NTOAD ; STORE MODIFIED ; ADDRESS XCHG ; SWITCH `TO` ; ADDRESS TO D REG LHLD NFROM ; FROM ADR. TO H DAD B ; ADD 8 TO `FROM` SHLD NFROM ; STORE MODIFIED ; ADDRESS LDA NGPAR ; PARAM. TO A REG JMP NGD1 ; JUMP TO CALL NGOUT: POP PSW RET ; RETURN ; ROUTINE TO ENCIPHER OR ; DECIPHER 8 BYTES, THE ; WORKING KEY MUST HAVE

Detailed Description Paragraph Table (10):

; PREVIOUSLY BEEN LOADED INTO ; THE ACTIVE KEY REGISTER. ; ADDRESS OF BYTES TO BE ; EN- OR DECIPHERED IN H & L ; REGISTER, ADDRESS IN WHICH ; TO PLACE RESULT IN D & E REG. ; PARAMETER IN A REG, ; ENCIPHER = 5H ; DECIPHER = 4H ; HAS PRGRAMMED DELAY > 320 ; MICROSEC. USES MOVE7 ; MVI A, PARAMETER ; LXI H, ADDR, DATA TO BE EN- ; OR DECIPHERED ; LXI D, ADDR, RESULTING 8 BYTE ; CALL EDCPR ; EDCPR: PUSH PSW PUSH B MVI B, OOH ; CLEAR B REG MOV C, A ; MOVE PARAM TO C SHLD TEMP2 ; STORE H TEMPO- ; RARILY LHLD BPARAM ; LOAD BPARAM IN ; H REG. DAD B ; ADD PARAM = 4H OR ; 5H TO BPARAM SHLD EDCP1 + 1 ; STORE RESULT IN ; OUT INSTRUCT. LHLD TEMP2 ; RESTORE H REG. IN BPARAM + REDST ; READ STATUS ORA A ; SET FLAGS EDER1: JNZ EDCP4 ; GO TO HALT CALL MOVE 7 ; FIRST 7 BYTES ; TRANSMITTED OUT EDCP1: OUT OOH ; 8th BYTE OUT LXI B, 500 ; COUNT TO B REG. EDCP2: CALL DELAY ; PROGRAMMED DELAY NOP ; > 320 MICROSEC IN BPRAM + REDST ; READ STATUS ORA A ; SET FLAGS EDER2: JM EDCP5 ; GO TO PARITY HLT EDER3: JNZ EDCP6 ; GO TO TIME OUT MVI B, 8H ; COUNTER TO B EDCP3: IN BPARAM + RDDAT ; READ NTH BYTE STAX D ; STORE NTH BYTE INX D ; INCR. ADDR DCR B ; DECR. COUNT JNZ EDCP3 ; LOOP POP B POP PSW RET ; RETURN EDCP4: HLT ; BUSY HALT EDCP5: HLT ; PARITY HALT EDCP6: HLT ; TIME OUT HALT ; MOVE7 SUBROUTINE TO MOVE ; FIRST 7 BYTES, USED BY LOAD ; WORKING KEY ROUTINE AND OTHER ; REQUIRES LEFT MOST ADDRESS ; IN H & L REGISTER, LXI H, ADR ; CALL MOVE 7 MOVE7: PUSH PSW PUSH B MVI B, 7 ; COUNT TO B REG MVE1: MOV A, M ; NTH BYTE TO A OUT BPARAM + WRTDAT ; WRITE NTH BYTE INX H ; INCR FROM ADDR DCR B ; DECR. COUNT JNZ MVE1 ; LOOP MV1 A, 50 ; PROGRAMMED MVE2: DCR A ; JNZ MVE2 ; DELAY IN BPARAM + REDST ; CHECK STATUS ORA A ; SET FLAGS MVER1: JM MVE3 ; PARITY ERROR HL MVER2: JNZ MVE4 ; TIME OUT HALT MOV A, M ; MOVE 8TH CHAR TO ; A REG FOR FINAL ; WRITE POP B POP PSW RET ; RETURN MVE3: HLT ; PARITY HALT MVE4: HLT ; TIME OUT HALT ; ; MAKE ODD PARITY, 8 BYTES, ; ADDRESS IN H & L ; LXI H, ADDR ; CALL MKODD MKODD: PUSH PSW PUSH B MVI B, 8H ; COUNT B MKD2: MOV A, M ; LOAD NTH BYTE ADI OOH ; SET PARITY FLAG JPO MKD1 ; IF PARITY IS ; ODD, SKIP 2 INST- ; RUCTIONS XRI 00000001B ; MAKE RITE MOST ; BIT ODD PARITY MOV M, A ; STORE NTH BYTE MKD1: INX H ; INCR ADDRESS DCR B ; DECR. COUNT JNZ MKD2 ; LOOP POP B POP PSW RET ; RETURN ; ROUTINE TO GENERATE MASTER ; KEY VARIANTS V1 OR V2 FROM ; MASTER KEY ; A REG CONTAINS PARAMETER TO ; SPECIFY WHICH VARIANT ; V1 = 01000001B ; V2 = 00001001B ; D & E CONTAINS ADDR OF VARIANT ; H & L ADDRESS OF MASTER KEY ; MVI A, PARAMETER ; LXI D, VARIANT (LOCATION) ; LXI H, MASTER KEY (LOCATION) ; CALL GNMKV GNMKV: PUSH PSW PUSH B STA GKV2 + 1 ; STORE PARAMETER ; IN INSTRUCTION MVI B, 8H ; COUNT TO B REG GKV1: MOV A, M ; LOAD NTH BYTE GKV2: XRI OOH ; MAKE VARIANT X, ; X = 1 OR 2 STAX D ; STORE NTH BYTE INX H ; INCR. FROM ADR. INX D ; INCR. TO ADDR. DCR B ; DECR. COUNT JNZ GKV1 ;LOOP POP B ; POP PSW ; RET ; RETURN ; WORKING KEY LOAD ROUTINE ; KEY DECIPHERED USING MASTER ; KEY WHICH MUST BE PREVIOUSLY ; LOADED IN MASTER KEY REG. ; WORKING KEY LOADED INTO ACT. ; REGISTER AFTER DECIPHERING ; USES MOVE7 ; LXI H, ADDR ADDRESS OF KEY ; CALL WKLOD WKLOD: PUSH PSW IN BPARAM + REDST ; CHECK STATUS ORA A ; SET FLAGS WKER1: JNZ WKL4 ; GO TO HALT CALL MOVE7 ; MOVE FIRST 7 BTE OUT BPARAM + DECWK ; 8TH BYTE OUT LXI B, 500 ; PROGRAMMED WKL1: CALL DELAY ; DELAY NOP ; > 320 MICROSEC. IN BPARAM + REDST ; CHECK STATUS ORA A ; SET FLAGS WHER2: JM WKL2 ; PARITY ERR.

HALT WKWE3: JNZ WKL3 ; TIME OUT HALT POP PSW ; RET ; RETURN WKL2: HLT ; PARITY ERR. HLT WKL3: HLT ; TIME OUT HALT WKL4: HLT ; BUSY HALT ; ROUTINE FOR PROGRAMMED ; DELAYS OF MORE THAN 255D ; INSTRUCTION EXECUTION ; TIMES SINCE A REG IS ; ONLY 8 BITS ; LXI B, COUNT > 255D ; CALL DELAY DELAY: PUSH PSW MOV A, C ; TRANSFER THE ADI OOH ; PART OF COUNT JZ DLY2 ; LESS THAN ; 255D TO A RG DLY1: DCR A ; DECR. A REG JNZ DLY1 ; < 255D LOOP DLY2: MV1 A, 254D ; SET UP 255 LOOP DLY3: DCR A ; DECR. A JNZ DLY3 ; 255D LOOP - DCR B ; DECR. 255 LOOP ; COUNT JNZ DLY2 ; LOOP ANOTHER ; 255 TIMES POP PSW RET ; RETURN ; ROUTINE TO MOVE N BYTES ; B REG = NO. OF BYTES ; D&E = TO ADDRESS ; H&L = FROM ADDRESS ; MAXIMUM 256 BYTES ; MVI B, NO. ; LXI D, TO ; LXI H, FROM ; CALL MOVEN MOVEN: PUSH PSW MVN1: MOV A, M ; LOAD NTH BYTE STAX D ; STORE NTH BYTE INX D ; INCR. TO ADDR. INX H ; INCR. FROM ADDR. DCR B ; DECR. COUNT JNZ MVN1 ; LOOP POP PSW ; RET ; RETURN ; COMPARE 2 FIELDS SUBROUTINE ; USED ONLY FOR DEBUGGING ; NO. OF BYTES IN B REG., ; ADDRESS OF ONE FIELD IN H, ; OTHER ADDRESS IN D ; MVI B, N ; LXI H, ADDR1 ; LXI D, ADDR2 ; CALL COMPR ; IF FIELDS ARE NOT EQUAL, ; ERROR HALT COMPR: PUSH PSW CMPR1: LDAX D ; ONE BYTE TO A CMP M ; COMPARE ONE BYTE CMPR2: JNZ CMPR3 ; IF NOT ZERO, HLT INX D ; INCR. D REG. INX H ; INCR. H REG. DCR B ; DECR. COUNT JNZ CMPR1 ; LOOP POP PSW RET ; RETURN CMPR3: HLT ; FROM CMPR2, HALT, ; 2 FIELDS NOT ; EQUAL ; ROUTINE TO DEBUG ALL OF ; OTHER ROUTINES, SIMULATES ; TERMINAL AND HPC. SENDS ; AND RECEIVES ONE MESSAGE ; AFTER GENERATING WK AND ; EITHER TK OR SP1. FINAL ; HALT AFTER TEST IS AT FINIS ; ERROR HALTS OTHERWISE. ; ROUTINE IS INITIATED AT ; `START` AND RUNS TO END. ; USES SUBROUTINE COMPR TO ; COMPARE RESULTS. ON NOT ; COMPARE, ERROR HALT AT CMPR3. START: STKLN 200D ; SET STACK = 200 LXI SP, STACK ; INITIALIZE STACK NOP NOP NOP

Detailed Description Paragraph Table (11):

NOP OUT BPARAM + RESET ; INITIALIZE DSM MVI A, 50 ; COUNT TO A REG. DBUG1: DCR A ; DECR. A JNZ DBUG1 ; LOOP - PROGRAMMED ; DELAY IN BPARAM + REDST ; READ STATUS ORA A ; SET FLAGS DBER1: JM DBUG4 ; PARITY ERROR DBER2 JNZ DBUG5 ; TIME OUT OR NOT ; READY ERROR MVI A, 5H ; PARAM = TERMINAL LXI H, ADRSP1 ; ADDR. OF FIRST OF ; 5 ADDRESS LIST ; TO H CALL MROUT ; DEBUG MAIN ROUT ; GENERATE WK & ; TK USING SP1 ; KMT, & TID MVI A, 3H ; PARAM = WORK KEY ; ACTIVE LXI H, DWK ; ADDR GENERATED ; WK CALL MWKLD ; SET WK ACTIVE MVI A, 5H ; PARAM = ENCIPH. MVI B, 4H ; ENCIPH. 4 EIGHT ; BYTE GROUPS LXI H, TMMSG ; ADDR. PLAIN TEXT ; TRANS. REQ. MSG. LXI D, TMEMSG ; SPACE FOR ENCIPH ; TRANS. REQ. MSG. CALL NGEDR ; ENCIPH TRM ; ; USING WK ; FIRST PART OF ROUTINE AS IF ; FROM TERMINAL COMPLETE, ; CONTINUE TO HPC ROUTINE ; JMP DEBUG2 ; CONTINUE DBUG2: MVI A, 4H ; PARAM = HPC LXI H, HADSP1 ; ADDR. OF FIRST ; OF 5 ADDRESS ; LIST TO H CALL MROUT ; DEBUG REST OF ; MAIN ROUTINE ; GENER. WK & SP1 ; USING TK, KMT, TID MVI B, 8H ; PARAM = LENGTH OF ; WK LXI H, HPCWK ; ADDR FIELD1 LXI D, DWK ; ADDR FIELD2 CALL COMPR ; COMPARE BOTH ; WK'S. HALT IF ; UNEQUAL. MVI B, 8H ; LENGTH OF SP1 LXI H, DSP1 ; ADDR FIELD 1 LXI D, HPSP1 ; ADDR FIELD 2 CALL COMPR ; COMPARE BOTH ; SP1'S. MVI A, 3H ; PARAM = WORK KEY ; ACTIVE LXI H, HPCWK ; ADDR WK TO H CALL MWKLD ; SET WK ACTIVE MVI A, 4H ; PARAM = DECIPH. MVI B, 4H ; DECIPH. 4 EIGHT ; BYTE GROUPS LXI H, TMEMSG ; CIPHER TRANS. ; REQ. MSG. LXI D, HPTRM ; SPACE FOR PLAIN ; TEXT TRANS. REQ ; MSG. CALL NGEDR ; DECIPHER TRM MVI B, 32 ; COUNT LXI H, HPTRM ; ADDR. FIELD 1 LXI D, TMMSG ; ADDR FIELD 2 CALL COMPR ; COMPARE TRM ; FROM TERMINAL ; AND FROM HPC. ; HALT ON ERROR MVI A, 5H ; PARAM = ENCIPH. MVI B, 3H ; ENCIPH. 3 EIGHT ; BYTE GROUPS LXI H, HRESP ; ADDR PLAIN TEXT ; RESPONSE MSG. LXI D, HENCR ; ADDR. LOCATION ; OF CIPHER ; RESPONSE MSG. CALL NGEDR ; ENCIPH. RESPONSE ; MSG. ; ; END OF HPC DEBUG, CONTINUE ; TO FINAL TERMINAL DEBUG ; JMP DBUG3 ; CONTINUE DBUG3: MVI A, 3H ; PARAM = WORK KEY ; ACTIVE LXI H, DWK ; ADDR WK CALL MWKLD ; SET WK ACTIVE MVI A, 4H ; PARAM = DECIPH

Detailed Description Paragraph Table (12):

MVI B, 3H ; DECIPH. 3 EIGHT ; BYTE GROUPS LXI H, HENCR ; CIPHER RESPONSE LXI D, DTMMS ; SPACE FOR PLAIN ; TEXT RESPONSE CALL NGEDR ; DECIPHER RESP. MVI B, 24 ; PARAM = RESPONSE ; MSG. LENGTH LXI H, DTMMS ; ADDR. FIELD 1 LXI D, HRESP ; ADDR. FIELD 2 CALL COMPR ; COMPARE 2 RES- ; PONSE MSGS. FINIS: HLT ; END OF ROUTINE ; DEBUG COMPLETE DBUG4: HLT ; PARITY ERROR ; HALT, FROM DBER1 DBUG5: HLT ; TIME OUT OR NOT ; READY HALT, ; FROM DBER2. END START ; END, TO START. ; PARAMETERS, LISTS, CONSTANTS ; ; ; BPARAM EQU 100H ; DSM BEGIN PARAM. MKEYL EQU 2H ; MASTER KEY LOAD WKEYL EQU 3H ; WORKING KEY LOAD DECDT EQU 4H ; DECIPHER DATA ENCDT EQU 5H ; ENCIPHER DATA DECWK EQU 6H ; DECIPHER WORK. KEY ENCWK EQU 7H ; ENCIPHER WORK. KEY RESET EQU 1H ; RESET DSM REDST EQU 2H ; READ STATUS TRMAK EQU 1H ; TRANSFER MAJOR KEY RDDAT EQU 4H ; READ DATA WRTDAT EQU 0H ; WRITE DATA WS1: DS 10 ; WORK STORE ADDR. LIST IADSP1 EQU WS1 ; INDIR. ADDR. SP1 IADTID EQU WS1 + 2 ; INDIR. ADDR TID IADKMT EQU WS1 + 4 ; INDIR ADDR KMT IADWK EQU WS1 + 6 ; INDIR ADDR WK IADTK EQU WS1 + 8 ; INDIR ADDR TK WS2: DS 120 ; WORK STORE SPARE EQU WS2 ; SPARE LOCATION KMT1 EQU WS2 + 8 ; KMT1 LOCATION KMT2 EQU WS2 + 16 ; KMT2 LOCATION TWK EQU WS2 + 24 ; TEMP WK TTK EQU WS2 + 32 ; TEMP TK SK EQU WS2 + 40 ; SK LOCATION DT1SK EQU WS2 + 48 ; D/KMT1/ (SK) DT2SK EQU WS2 + 56 ; D/KMT2/(SK) SP2 EQU WS2 + 64 ; SP2 LOCATION SP3 EQU WS2 + 72 ; SP3 LOCATION TEMP1 EQU WS2 + 80 ; TEMP LOCATION TEMP2 EQU WS2 + 88 ; TEMP LOCATION TEMP3 EQU WS2 + 96 ; TEMP LOC. TEMP4 EQU WS2 + 104 ; TEMP LOC. MRPAR EQU WS2 + 112 ; TEMP EN/DE PAR KMT: DB

1301H ; DUMMY KMT, BEFORE DB 1301H ; DEBUGGING, MUST DB 1301H ; BE MADE EQUAL TO DB 1301H ; D/KMO/(EKMT) ; THIS VALUE IS ; USED FOR DEBUG. ; AS IF FROM TERM. WS3: DS 6 ; WORK STORE NGPAR EQU WS3 ; STORE EN/DE/ ; CIPHER PARAMET. NGRPS EQU WS3 + 1 ; STORE N GROUPS NFROM EQU WS3 + 2 ; STORE FROM ADR. NTOAD EQU WS3 + 4 ; STORE TO ADDR. ; FOR DEBUGGING ONLY ; KMO: DB EFEFH ; DUMMY DB EFEFH ; MASTER DB EFEFH ; KEY DB EFEFH ; EKMT: DB EOEOH ; DUMMY DB EOEOH ; ENCRYPTED DB EOEOH ; TERMINAL DB EOEOH ; KEY DTID: DB 0101H ; DUMMY DB 0101H ; DB 0101H ; TID DB 0101H ; DWS: DS 16 ; DEBUG LOCATIONS DWK EQU DWS ; DUMMY W:K LOC DTK EQU DWS + 8 ; DUMMY TK LOC DSP1: DB 1010H ; DUMMY DB 1010H ; SP1 DB 1010H ; PARAMETER DB 1010H ; ADRSP1: DW DSP1 ; ADDR OF SP1 ADRTID: DW DTID ; ADDR OF TID ADRKMT: DW KMT ; ADDR OF KMT ADRWK: DW DWK ; ADDR OF WK ADRTK: DW DTK ; ADDR OF TK ; THE ABOVE LIST IS ; USED FOR TERMIN. ; DEBUGGING TMMSG: DB `IMPORTAN` ; TRANSACTION REQ. DB `T MESSAG` ; MSG. USED AT DB `E to FOL` ; TERM., WILL BE DB `LOW SOON` ; ENCIPH. BY WK DTMMS: DB 24 ; AREA FOR ENCIPH. ; TRANS. REQ. MSG. ; RESPONSE FROM ; HPC AFTER DECIPH. HPCWK: DS 8 ; AREA IN WHICH TO ; STORE WK GENERATED ; AT DUMMY HPC, ; CHECK AGAINST DWK HPSP1: DS 8 ; AREA FOR SP1 ; FROM DUMMY HPC ; CHECK AGAINST DSP1 HPTRM: DS 32 ; AREA FOR DECIPH ; TRANS. REQ. MSG. ; FROM HPC, CHECK ; AGAINST TMMSG HRESP: DB `DISREGAR` ; RESPONSE MSG., DB `D FIRST` ; WILL BE ENCIPH. DB `MESSAGEX` ; BY HPC USING WK HENCR: DS 24 ; AREA FOR ENCIPH ; RESPONSE MSG., ; USED AT HPC HADSP1: DW HPSP1 ; SP1 LOCATION HADTID: DW DTID ; TID LOC. HADKMT: DW EKMT ; ENCIPH. KMT LOC. HADWK: DW HPCWK ; HPC-WK LOC. HADTK: DW DTK ; TK LOC. TMEMSG: DS 32 ; AREA FOR ENCRYP- ; TED TRANS. REQ. ; MSG. FROM TERM.

Current US Class (3):
705

CLAIMS:

1. In a system for authenticating users and devices in on-line transaction networks comprising a plurality of remote terminals in communication with a central processing unit including a data base containing encrypted data used in the authentication of the users and devices, said data being encrypted with a master key and including terminal master keys for each of said remote terminals and identification numbers for each of said users all of which are secret, said data further including terminal identification numbers for each of said remote terminals and account numbers for each of said users, wherein each of said remote terminals is provided with means for entering an account number and an identification number of a user initiating a transaction as well as the nature of the transaction, the improvement in a method for protecting the transaction comprising the steps of:

generating at a terminal a transaction request message based on the information entered at the terminal by a user initiating a transaction,

using the identification number and the account number entered by the user and the terminal identification number and the terminal master key, and employing such variants as to generate a working key unique to each transaction,

encrypting the transaction request message using the working key,

transmitting the encrypted transaction request message,

deriving the working key at the central processing unit using information derived from the transmitted message and the data base including the account number, the terminal master key and the terminal identification number,

decrypting the message received at the central processing unit using the working key,

comparing the user identification number and account number obtained by decrypting corresponding data in the data base with the data in the transaction request message to validate the transaction request message,

generating a transaction request response and encrypting the transaction request response with the working key,

transmitting the encrypted transaction request response to the terminal where the transaction was initiated, and

decrypting the message received at the terminal using the working key and, if the transaction is approved, providing the requested service.

2. The method of protecting a transaction as recited in claim 1, further comprising the step of appending the account number to the encrypted transaction request message prior to transmitting and wherein the step of deriving the working key is performed by generating the working key using the appended account number, the user identification number, the terminal identification number and the terminal master key.

3. The method of protecting a transaction as recited in claim 1, further comprising the steps of generating a transmitted key using the working key and appending the transmitted key to the encrypted transaction request message prior to transmitting and wherein the step of decrypting the message is performed using the appended transmitted key to obtain the working key, the working key then being decrypted to obtain the user identification number.

4. The method of protecting a transaction as recited in claim 3, further comprising the steps of:

after decrypting the message received at the terminal, generating and transmitting an acknowledgement to the central processing unit, and

destroying the working key at the terminal and the central processing unit after acknowledgement.

5. The method of protecting a transaction as recited in claim 4, wherein said acknowledgement is encrypted using the working key.

6. The method of protecting a transaction as recited in claim 3, wherein the step of generating the working key comprises the steps of:

using the user identification number and account number entered at the terminal, generating a first security parameter,

generating a secondary key by encoding the terminal identification number using the terminal master key, and

using the first security parameter and the secondary key to generate the working key.

7. The method of protecting a transaction as recited in claims 3 or 6, wherein the time of day is also used to generate the working key.

8. The method of protecting a transaction as recited in claim 6, wherein the time of day is used to generate the first security parameter and at the central processing unit, further comprising the step of decrypting the first security parameter using the working key to obtain the time of day, the transaction not being approved if the decrypted time of day varies by more than a predetermined time period from the time of day at the central processing unit.

9. The method of protecting a transaction recited in claim 4, further comprising the step of updating the data base at the central processing unit after acknowledgement.

10. The method of protecting a transaction as recited in claim 3, wherein each of said terminals includes a card reader for reading a user card encoded with the user account number, the card being inserted in the card reader in order to initiate a transaction and the user then entering a user identification number.

11. The method of protecting a transaction as recited in claim 10, wherein the card encoded with the user account number also has an anti-counterfeiting feature, and the step of generating a working key comprises the steps of:

using the user account number and identification number, the anti-counterfeiting feature and the time of day, generating a first security parameter,

generating a secondary key by encoding the terminal identification number using the terminal master key, and

using the first security parameter and the secondary key to generate the working key.

12. The method of protecting a transaction as recited in claim 6, wherein the step of generating the working key further comprises the steps of:

using the first security parameter and the secondary key, generating a second security parameter, and

using the second security parameter and the secondary key to generate the working key.

13. The method of protecting a transaction as recited in claim 12, wherein the step of generating the transmitted key comprises the steps of:

generating a third security parameter using the working key and the secondary key, and

generating the transmitted key using the third security parameter and the secondary key.

14. The method of protecting a transaction as recited in claim 13, wherein the step of decrypting the message received at the central processing unit comprises the steps of:

multiply decrypting the transmitted key to first obtain the third security parameter and then the working key, and

decrypting the transaction request message using the decrypted working key.

15. The method of protecting a transaction as recited in claim 10, wherein after the step of comparing the user identification number and account number, if the transaction is not validated, comprising the further step of requesting that the user identification number be re-entered to re-initiate the transaction.

16. The method of protecting a transaction as recited in claim 15, wherein the card is retained in the card reader and not returned to the user if the step of requesting the user identification to be re-entered is repeated a predetermined number of times.

17. The method of protecting a transaction as recited in claim 3, wherein the on-line transaction networks comprise a plurality of central processing units each in communication with other central processing units, each of said central processing units having an identification number which is used to obtain a secret interchange master key and a secret password, further comprising the steps in an interchange transaction between central processing units of:

using the interchange master key and the password to generate an interchange working key,

encrypting the terminal identification number and the terminal master key using the interchange working key to generate an interchange transmitted key and appending the interchange transmitted key to the encrypted transaction request message, and

transmitting the encrypted transaction request message with the appended interchange transmitted key to a second central processing unit.

Previous Doc Next Doc Go to Doc#